НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

Інститут телекомунікаційних систем

Кафедра Інформаційно-телекомунікаційних мереж

До захисту допущено:

Завідувач кафедри

_____ Лариса ГЛОБА

«___»_____2020 р.

Дипломна робота

на здобуття ступеня бакалавра

за освітньо-професійною програмою «Інформаційно-комунікаційні технології»

спеціальності 172 «Телекомунікації та радіотехніка»

на тему: «Аналіз використання протоколів IPSec для підвищення рівня інформаційної безпеки»

Виконала:
студентка IV курсу, групи ТІ- 61
Турчин Яна Василівна _____

Керівник:
доцент кафедри ІТМ ІТС, к.т.н.
Кононова Ірина Віталіївна _____

Рецензент:
старший викладач кафедри ТС ІТС,
Вакуленко Олександр Володимирович _____

Засвідчую, що у цій дипломній роботі немає запозичень з праць інших авторів без відповідних посилань.
Студентка _____

Київ – 2020 року

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Інститут телекомунікаційних систем
Кафедра Інформаційно-телекомунікаційних мереж

Рівень вищої освіти – перший (бакалаврський)

Спеціальність – 172 «Телекомунікації та радіотехніка»

Освітньо-професійна програма «Інформаційно-комунікаційні технології»

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Лариса ГЛОБА
«___»_____2020 р.

ЗАВДАННЯ
на дипломну роботу студенту
Турчин Яні Василівні

1. Тема роботи «Аналіз використання протоколів IPSec для підвищення рівня інформаційної безпеки», керівник роботи доцент кафедри інформаційно-телекомунікаційних мереж ІТС, к.т.н., Кононова Ірина Віталіївна, затверджені наказом по університету від «30» березня 2020 р. № 924-с

2. Термін подання студентом роботи 8 червня 2020 р.

3. Вихідні дані до роботи:

1.Спеціальна література, матеріали мережі інтернет

2.Наукові статті про підвищення рівня інформаційної безпеки

3.Використання протоколів IPSec для захисту даних

4. Зміст роботи:
1. Проблеми забезпечення інформаційної безпеки в мережах з пакетною передачею даних

2. Аналіз набору протоколів IPsec, що забезпечують захист даних, які передаються за допомогою протоколу IP

3. Рекомендації налаштування параметрів безпеки набору протоколів IPsec на мережному обладнанні Cisco

5. Перелік ілюстративного матеріалу (із зазначенням плакатів, презентацій тощо):

- Титульний слайд
- Мета, актуальність
- Напрями забезпечення інформаційної безпеки та порівняння основних технологій захисту
- IPSec та протоколи безпеки
- Варіанти застосування IPSec та формати IP пакетів у різних режимах роботи
- Схеми тестування швидкодії протоколу IPSec в емуляційному програмному середовищі та на реальному обладнанні
- Результати досліджень
- Загальні висновки

6. Дата видачі завдання 10 вересня 2020 р.

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання етапів роботи	Примітка
1	Підготовка і вивчення літератури	до 25.09.2020	Виконано
2	Розробка вступу	До 23.02.2020	Виконано
3	Розробка 1 розділу	До 15.03.2020	Виконано
4	Розробка 2 розділу	До 01.04.2020	Виконано
5	Розробка 3 розділу	До 12.05.2020	Виконано
6	Підготовка доповіді	До 08.06.2020	Виконано
7	Оформлення роботи	До 08.06.2020	Виконано

Студент Яна ТУРЧИН

Керівник Ірина КОНОНОВА

РЕФЕРАТ

Дипломна робота «Аналіз використання протоколів IPsec для підвищення рівня інформаційної безпеки» складається з переліку умовних скорочень, вступу, основної частини, що містить 3 розділи, висновків і списку використаних джерел. Загальний обсяг роботи – 77 сторінок. Робота містить 47 рисунків та 2 таблиці. Список використаних джерел включає 29 одиниць.

У відповідності до мети дослідження, в даній роботі названі різні способи забезпечення інформаційної безпеки в мережі Інтернет і дано докладний аналіз використання протоколів IPSec для цієї мети. Проведені дослідження ефективності роботи протоколів IPSec і впливу використання цих протоколів на швидкість передачі даних в мережі. Дослідження впливу цих протоколів на швидкість передачі та навантаження проводилось у віртуальному середовищі EVE-NG та на реальному обладнанні Cisco.

Ключові слова: протокол IPSec, безпека мереж з пакетною передачею даних, інформаційна безпека, захист інформації, оцінка якості та захищеності.

ABSTRACT

Diploma work "Analysis of the use of IPsec protocols to increase the level of information security" consists of a list of abbreviations, introduction, main part, containing 3 sections, conclusions and a list of sources used. Total work – 77 pages. The work contains 47 figures and 2 tables. The list of used sources includes 29 units.

In accordance with the purpose of the study, in this paper, the different ways of ensuring information security in the Internet are named and a detailed analysis of the use Of IPSec protocols for this purpose is given. The efficiency of IPSec protocols and the impact of the use of these protocols on the speed of data transmission in the network are studied.The study of the impact of these protocols on the transfer rate and load was conducted in the virtual environment of EVE-NG and on real Cisco equipment.

Keywords: IPSec protocol, security of packet data networks, information security, information security, quality and security assessment.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

АРМ	автоматизоване робоче місце
АС	автоматизована система
МЕ	міжмережевий екран
НСД	несанкціонований доступ
ПЗ	програмне забезпечення
ПК	персональний комп’ютер
3DES	(Triple Data Encryption Standard) – симетричний блочний шифр
ACL	(Access list) – список управління доступом
AES	(Access list) – список управління доступом
AH	AES (Advanced Encryption Standard) – симетричний алгоритм блочного шифрування
CLI	(Command-line interface) – різновид текстового інтерфейсу
DES	(Data Encryption Standard) – симетричний алгоритм шифрування
DH	(Diffie–Hellman) – криптографічний протокол
ESP	(Encapsulating Security Payload) – протокол забезпечення безпеки трафіку
HMAC	(Hash-based message authentication code) – механізм перевірки цілісності даних
HTTP	(Hyper Text Transfer Protocol) – протокол передачі даних
IANA	(Internet Assigned Numbers Authority) – функція керування просторами IPSec
ICMP	(Internet Control Message Protocol) – мережевий протокол
IETF	(Internet Engineering Task Force) – міжнародне співтовариство
ICV	(Ntegrity Check Value) – алгоритм перевірки даних
IKE	(Internet Key Exchange) – протокол набору протоколів IPSec
IOS	(Internetwork Operating System) – міжмережева операційна система
IP	(Internet Protocol) – протокол міжмережевого рівня
IPSec	(IP Security) – набір протоколів для захисту даних

ISAKMP (Internet Security Association and Key Management Protocol – протокол TCP/IP стеку

L2TP (Layer 2 Tunneling Protocol) – протокол тунелювання другого рівня

MD5 (Message Digest 5) – алгоритм хешування

OSPF (Open Shortest Path First) – протокол динамічної маршрутизації

PKI (Public Key Infrastructure) – метод забезпечення криптозадач

RFC (Request for Comment) – документ Інтернету, що містить технічні стандарти

RSA (Rivest, Shamir, Adleman) – криптографічний алгоритм з відкритим ключем

SA (Security Association) – асоціація безпеки

SAD (Security Associations Database) – база даних асоціації безпеки

SHA (Secure Hash Algorithm) – алгоритм безпечного хешу

SMTP (Simple Mail Transfer Protocol) – протокол пересилання пошти

SOCKS (SOCKet Secure) – фреймова структура

SPD (Security Policy Database) – база даних політики безпеки

SPI (Security Parameters Index) – ідентифікаційний тег

SSH (Secure Shell) – мережевий протокол прикладного рівня

SSL (Secure Sockets Layer) – протокол безпеки на транспортному рівні

TCP (Transmission Control Protocol) – протокол передачі даних

TLS (Transport Layer Security) – криптографічний протокол

UDP (User Datagram Protocol) – протокол в стеку TCP/IP

ULP (Up-level protocol) – протокол верхнього рівня

VPN (Virtual Private Network) – віртуальна приватна мережа

ВСТУП

Сфера інформаційних технологій вже повністю увійшла в усі сфери людської діяльності. Всесвітня мережа Інтернет вже об’єднала не тільки корпоративні мережі, а й окремих користувачів зі своїми персональними комп’ютерами та смартфонами. Усе це можливо завдяки стеку протоколів TCP/IP, які лежать в основі мережі.

Проблема захисту переданої інформації від несанкціонованого доступу або спотворення хвилює багатьох користувачів, яким необхідно мати постійний доступ до своєї персональної інформації і бути впевненими в неможливості її неправомірного використання.

Найбільш гостро ця проблема стоїть перед державними службами і організаціями. При появі загроз, пов'язаних з можливістю втрати, спотворення, розкриття конфіденційних даних і витоку стратегічно важливої інформації, організація або держава в цілому може втратити не тільки величезні суми грошей, але і репутацію на політичному та економічному рівні.

Домогтися високого ступеня захищеності можна тільки при використанні передових технологій захисту мережі передачі даних.

З розвитком технологій підвищується і рівень загроз для використаних інформаційних технологій. З кожним роком з'являються все нові і нові атаки на мережі передачі даних. У відповідь на нові атаки з'являються нові або удосконалюються старі методи захисту інформації та інформаційно-технічної інфраструктури.

За допомогою використання сучасних способів і засобів захисту цілісності та конфіденційності інформації (антивірусних програм, міжмережевих екранів, програмних і апаратних продуктів для захисту

інформації від НСД, вірусних атак та інших загроз) можна забезпечити безпеку автоматизованої системи в цілому і особистого автоматизованого робочого місця (АРМ) користувача.

Успіх застосування систем захисту інформації залежить від наявності у них розвинених засобів керування режимами роботи і реалізації функцій, що дозволяють

істотно спростити процеси встановлення, налаштування та експлуатації засобів захисту.

У даній роботі названі різні способи забезпечення інформаційної безпеки в мережі Інтернет і дано докладний аналіз використання протоколів IPSec для цієї мети. Проведені дослідження ефективності роботи протоколів IPSec і впливу використання цих протоколів на швидкість передачі даних в мережі.

Актуальність і перспективність полягає в наступному. Проблема захисту інформації від несанкціонованого доступу або спотворення найбільш гостро стоїть перед усіма сучасними організаціями. Технологія IPSec є однією з технологій, що вирішують дану проблему.

Таким чином, ***об'єктом досліджень*** є проблеми забезпечення інформаційної безпеки в мережі з пакетною передачею даних.

Предмет досліджень – набір протоколів IPsec, які забезпечують захист даних, що передаються за допомогою протоколу IP.

Мета досліджень – проаналізувати всі можливі варіанти сполучень технологій протоколу IPsec в емуляційному програмному середовищі та на реальному обладнанні.

Наукова новизна дослідження – аналіз застосування різних комбінацій протоколів IPSec і їх вплив на якість та захищеність передачі даних в мережі.

РОЗДІЛ 1.

ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В МЕРЕЖІ З ПАКЕТНОЮ ПЕРЕДАЧЕЮ ДАНИХ

1.1 Аспекти забезпечення інформаційної безпеки у відомчих мережах

Галузь інформаційних технологій удосконалюється у дуже швидкому темпі, нові технології, ідеї, винаходи виникають у світі кожного дня, а також способи їх застосування для покращення людського життя. Проблеми інформатизації суспільства вирішуються на державному рівні, уряди стурбовані рівнем інформатизації всіх верств і категорій населення, приймається безліч законів про запровадження інформаційних нововведень у всі сфери людської діяльності.

Зараз вже складно уявити життя без мобільних телефонів, електронної пошти, цікавих і корисних мережевих додатків, мережевого спілкування, можливості термінових ділових переговорів або важливої інформації через Інтернет в будь-якому місці, де б не виникла така необхідність, без обмежень в часі і в просторі.

Інформаційні технології впевнено проникають в наше життя, а відтак все більше відомостей про нас, які знаходяться в мережі, необхідно захищати.

Електронні щоденники та журнали, електронні медичні картки, віртуальні банки, які надають можливість проведення банківських операцій через мережу, електронні гроші і платежі, що надають можливість оплати покупок і послуг через Інтернет, все це зручні нововведення, але вони ж являють собою потенційну небезпеку, і можуть бути причиною вторгнення в особисте життя кожної людини.

Всі ці нововведення вимагають особливої уваги до конфіденційності інформації. При недостатній увазі до цієї проблеми зловмисник легко зможе отримати інформацію про стан здоров'я будь-якої людини, атрибути його банківської карти, облікові записи соцмереж і електронної пошти, паспортні дані, бази і списки клієнтів будь-якої організації, фінансові дані громадян та пошкодити або використовувати цю інформацію в своїх цілях.

Для користувачів, змушених використовувати Інтернет в якості сховища своїх персональних даних, дуже важливо бути впевненими в тому, що інформація, власниками якої вони є, не буде отримана несанкціонованими користувачами.

З розвитком інформаційних і комп'ютерних технологій, без забезпечення інформаційної безпеки стало неможливо існування дрібних і великих компаній і організацій. На сьогоднішній день ключову роль в забезпеченні ефективного виконання бізнес – процесів як комерційних, так і державних установ відіграють автоматизовані системи (АС). Разом з тим повсюдне використання АС для зберігання, передавання і переробки даних призводить до підвищення актуальності проблем, пов'язаних з їх захистом. Підтвердження цього можна отримати із статистичних даних, які показують, що як в Україні, так і в інших розвинутих закордонних країнах має місце тенденція збільшення кількості інформаційних атак, що призводять до значних фінансових і матеріальних втрат [1].

Майже кожна АС може бути об'єктом інформаційного нападу. Для реалізації атаки порушнику необхідно активізувати або, іншими словами, використовувати деяку вразливість АС, тобто слабке місце АС, на основі якого можлива успішна реалізація атаки.

Прикладами вразливостей АС можуть бути: експлуатація нестійких до викриття паролів, присутність оновлення без потрібних модулів, некоректна зміна мережевої служби АС, дефіцит потрібних ресурсів захисту інформації та ін.

На сьогоднішній день рівень захищеності від можливих загроз на пряму впливає на продуктивну роботу установ на підприємств, які використовують певні системи передачі інформації. Якщо організація не може бути впевнена, що її конфіденційна інформація захищена від витоку або пошкодження, їй варто відмовитися від використання інфо-комунікаційних послуг, що в умовах сучасної економіки практично нереально, так як неминуче призведе до втрати можливості швидко реагувати на зміни ринку, а отже, до втрати конкурентоспроможності.

Тому сучасним підприємствам необхідно використовувати автоматизовані системи і мережі передачі даних і бути впевненими, що інформаційна безпека надійно забезпечена.

Крім попиту комерційних підприємств на мережеві послуги, зростає і число користувачів мережі Інтернет, кожен з яких може бути ініціатором хакерських атак або їх жертвою. Доступ до даних в Інтернет може отримати абсолютно будь-який користувач, якщо ці дані не захищені відповідним чином, і навмисно пошкодити, знищити або перехопити і використовувати їх у своїх цілях. Крім того дані можуть бути пошкоджені ненавмисно, через помилки в програмному забезпеченні, технічні збої в мережі. Все це являє собою серйозну загрозу безпеці користувальницьких даних.

Домогтися високого ступеня захищеності можна тільки, якщо використовувати передові технології захисту мережі передачі даних. Внаслідок поширення і збільшення доступності мережевих технологій, служби забезпечення безпеки стали важливою частиною роботи мережі.

Отже, коли є необхідність працювати в інформаційному просторі і передавати дані через загальнодоступні мережі, такі як Інтернет, виникає гостра потреба у надійному захисті інформації. Це дозволяє стверджувати, що проблема захисту інформації сьогодні є актуальною та важливою.

1.2 Комплексний підхід до забезпечення інформаційної безпеки

Комплексний підхід до забезпечення інформаційної безпеки передбачає координоване застосування програмних, організаційних і технічних заходів, які у свою чергу блокують канали вірусних загроз. Відповідно до цього способу організація повинна впровадити сукупність дій:

- заходи щодо виявлення і усунення вразливостей, після аналізу яких, з’являються загрози. За допомогою цього можна позбутися інформаційних атак;
- заходи, спрямовані на своєчасне виявлення і запобігання інформаційних атак;
- заходи, що забезпечують виявлення та усунення наслідків атак.

Саме ці заходи захисту спрямовані на мінімізацію втрати, завданої в результаті впровадження загроз безпеки [2-3].

Потрібно розуміти, що ефективна реалізація згаданих вище способів на підприємстві можлива тільки за умови наявності нормативно-методичного, технологічного та кадрового забезпечення інформаційної безпеки, рис. 1.1.

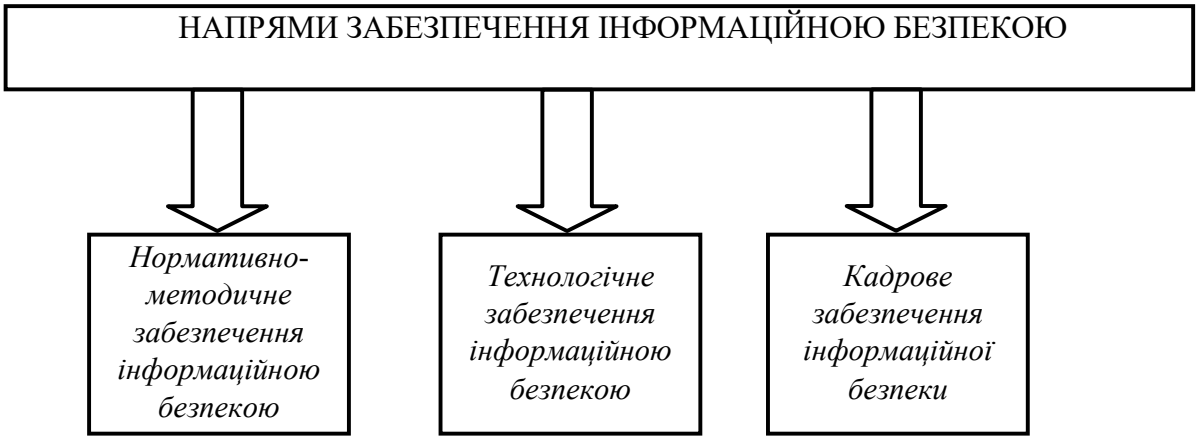

Рис. 1.1 Основні напрями забезпечення інформаційної безпеки

Найбільша ефективність буде отримана у разі застосування комплексного захисту з перерахованих вище способів.

Нормативно-методичне забезпечення інформаційною безпекою передбачає введення злагодженої правової бази у сфері захисту від загроз. Організаційні засоби захисту пов'язані з розробкою і впровадженням на підприємствах нормативно-правових документів, що визначають вимоги до інформаційної безпеки, такі як політика і концепція забезпечення інформаційної безпеки, посадові інструкції по роботі персоналу з АС і т.д [2].

В рамках кадрового забезпечення інформаційної безпеки в компанії повинен бути організований процес навчання працівників з питань протидії інформаційним атакам.

Програмно-технічні засоби забезпечення інформаційної безпеки є основою системи захисту інформації. Це сукупність алгоритмів, програм і протоколів, що забезпечують шифрування, контроль за НСД, захист від шкідливих програм і багато іншого.

На сьогоднішній день можна виділити наступні основні види технічних засобів захисту:

- засоби криптографічного захисту інформації;
- засоби розмежування доступу користувачів до ресурсів АС;
- засоби міжмережевого екранування;
- засоби аналізу захищеності АС;
- засоби викриття атак;
- засоби антивірусного захисту;
- засоби аналізу контенту;
- засоби захисту від спаму.

Засоби криптографічного захисту інформації являють собою засоби обчислювальної техніки, що здійснюють криптографічне перетворення інформації для забезпечення її конфіденційності та контролю цілісності.

Засоби розмежування доступу призначені для захисту від неправомірного доступу до інформаційних складових системи. Розмежування доступу виконується засобами захисту на основі процедур ідентифікації, автентифікації та авторизації користувачів, які претендують на отримання доступу до інформаційних ресурсів АС, рис. 1.2.

Рис. 1.2 Процедура входу користувача в автоматизовану систему

Міжмережеві екрани відповідають за реалізацію методів контролю за інформаційними даними, що надходять в АС і/або виходить з АС, та за забезпечення захисту АС за допомогою фільтрування інформації на основі параметрів, заданих адміністратором. Процес фільтрування включає в себе аналіз заголовків кожного з

пакетів, що проходить через МЕ, і передачу його далі за маршрутом прямування тільки в разі, якщо він задовольняє усі задані правила фільтрування. За допомогою фільтрації МЕ можливе забезпечення захисту від мережевих атак шляхом видалення з інформаційного потоку саме тих пакетів даних, які являються потенційно небезпечними для АС [4-5].

Засоби аналізу захищеності призначені для пошуку вразливих місць у програмно-апаратному забезпеченні АС [4-5].

Системи виявлення атак являють собою спеціалізовані програмні або програмно-апаратні комплекси, призначені для виявлення інформаційних атак на ресурси АС за допомогою збору та аналізу даних про події, що реєструються в системі.

Засоби антивірусного захисту призначені для виявлення і видалення шкідливого ПЗ, присутнього в АС. До таких шкідливих програм відносяться комп'ютерні віруси, а також ПЗ типу «троянський кінь», «spyware».

Засоби захисту від спаму забезпечують виявлення і фільтрацію незапрошених поштових повідомлень рекламного характеру. У ряді випадків для розсилки спаму використовується шкідливе ПЗ, впроваджуване на хости АС і використовує адресні книги, які зберігаються в поштових клієнтах користувачів.

Засоби аналізу контенту призначені для моніторингу мережного трафіку з метою виявлення порушень політики безпеки. В даний час можна виділити два основних види засобів аналізу контенту – системи аудиту поштових повідомлень і системи моніторингу Інтернет-трафіку. Системи аудиту поштових повідомлень припускають збір інформації про SMTP-повідомлення, що циркулюють в АС, і її наступний аналіз із метою виявлення несанкціонованих повідомлень, що порушують вимоги безпеки, задані адміністратором. Так, наприклад, системи цього типу дозволяють виявляти і блокувати можливі канали витоку конфіденційної інформації через поштову систему.

Системи моніторингу Інтернет-трафіку призначені для контролю доступу користувачів до ресурсів мережі Інтернет. Засоби захисту даного типу дозволяють обмежити доступ користувачів до заборонених Інтернет-ресурсів, а також виявити

спробу передачі конфіденційної інформації по протоколу HTTP. Системи моніторингу встановлюються таким чином, щоб через них проходив весь мережевий трафік, що передається в мережу Інтернет.

Для використання сервісів безпеки можуть реалізувати такі механізми та їх сполучення:

1) шифрування відповідає за кодування інформації. Іншими словами це процес перетворення початкової інформації (простого тексту) в іншу форму, а саме в шифрований текст. Тільки довірені сторони мають змогу розшифрувати шифротекст та отримати оригінальну інформацію;
2) електронний цифровий підпис – дані, які додаються до інших даних та документів в електронній формі. Відповідає за ідентифікацію автора та має аналогічну юридичну силу, як і звичайний підпис;
3) механізми керування доступом – комплекс способів для надання певних повноважень та регулювання прав доступу;
4) механізми контролю цілісності даних відповідають за достовірність, точність та цілісність даних при їх обробці та збереженні;
5) механізми автентифікації – процес перевірки належності інформації користувачу за допомогою певного ідентифікатора;
6) механізми додаткового трафіку допомагають зробити аналіз трафіку важчим;
7) механізми керування маршрутизацією – відповідають за встановлення шляху, яким будуть проходити потоки інформаційних даних;
8) механізми нотаризації – служать для підтвердження таких складових комунікації, як особи відправника, часу, цілісності інформації. Крім відправника і отримувача є третя сторона, яка володіє достатньою кількістю інформації. В загальному випадку механізм нотаризації опирається на механізм цифрового підпису [6].

1.3 Протоколи безпеки у мережах з пакетною передачею даних

В Інтернет вже давно існує цілий ряд комітетів, які займаються стандартизацією всіх інтернет-технологій. Ці організації, які складають основну частину Робочої групи інженерів Інтернету (IETF), вже стандартизували кілька важливих протоколів, тим самим прискоривши їх впровадження в мережі.

Secure Socket Layer (SSL) та Secure Shell (SSH) протоколи безпеки, що працюють на транспортному рівні. Вони відповідають за забезпечення безпечної передачі даних між сервером та клієнтом. Ці протоколи були розроблені робочою групою IETF з безпеки транспортного рівня (Transport Layer Security – TLS). Безпечний протокол передачі гіпертексту (S-HTTP) надає надійний механізм web-транзакцій.

Засіб SOCKS є фреймовою структурою, що дає можливість додаткам клієнт/сервер в доменах TCP і UDP зручно і безпечно користуватися послугами міжмережевого екрану. IP (IPSec) – протокол безпеки представляє собою набір стандартів підтримки конфіденційності та цілісності даних на мережевому рівні (в мережах IP). X.509 – це стандарт безпеки і автентифікації, який підтримує структури безпеки електронного інформаційного транспорту. Саме за допомогою нього визначається структура даних цифрового сертифіката і вирішується питання звернення загальних ключів. X.509 являється найважливішим компонентом інфраструктури загальних ключів (PKI) [7-8].

IPSec та SSL (TLS) являються найбільш популярними протоколами захищеної передачі даних в мережі Інтернет.

SSL (TLS) – найвідоміший протокол шифрування даних на мережевому рівні. Являє собою набір криптографічних алгоритмів, методів і правил їх застосування. За допомогою SSL можна встановлювати захищене з'єднання, здійснювати контроль цілісності даних і вирішувати різноманітні супутні завдання [9].

IPSec – рада по архітектурі Інтернету (IAB) випустила звіт «Безпека архітектури Інтернет». У цьому документі розглянуто основні області застосування додаткових засобів безпеки у мережі Інтернет, а саме захист від неправомірного

моніторингу, підміни пакетів та керування потоками даних. У числі першочергових і найбільш важливих захисних заходів названа необхідність планування концепції та основних способів забезпечення конфіденційності та цілісності потоків даних.

Так як зміна стандартних протоколів сімейства TCP/IP викликала б повну перебудову мережі Інтернет, було поставлено завдання забезпечення безпеки інформаційного обміну у відкритих телекомунікаційних мережах на базі існуючих протоколів.

Таким чином, почала створюватися специфікація Secure IP, додаткова у відношенні до протоколів IPv4 та входить в стандарт IPv6. Специфікація розробляється робочою групою IP Security IETF. На сьогоднішній день IPSec включає три алгоритмо-незалежних стандартних специфікації, що представляють собою відповідні RFC-стандарти. Протокол IPSec дозволяє забезпечити базовий спосіб шифрування трафіку на мережевому рівні та захищає інформацію на основі наскрізного шифрування: незалежно від працюючого додатка, шифрується кожен пакет даних, що проходить по каналу. Саме це дає змогу організаціям створювати в Інтернеті приватні віртуальні мережі. Протокол IPSec працює поверх звичайних протоколів зв'язку, підтримуючи AES, SHA і ряд інших криптографічних алгоритмів [7-10].

Забезпечення інформаційної безпеки на мережевому рівні з допомогою IPSec включає:

- підтримку немодифікованих кінцевих систем;
- підтримку транспортних протоколів, відмінних від TCP;
- підтримку віртуальних мереж в незахищених мережах;
- захист заголовка транспортного рівня від перехоплення (захист від несанкціонованого аналізу трафіку);
- захист від атак типу «відмова в обслуговуванні».

Окрім цього, протокол IPSec має дві важливі переваги:

- його використання не вимагає змін в проміжних пристроях мережі;
- робочі місця і сервери не обов'язково повинні підтримувати IPSec.

IPSec – це рішення Cisco, Nokia. Не дивлячись на досить велику кількість різноманітних рішень, всі вони добре поєднуються один з одним [9-11].

Порівняння протоколів IPSec і SSL представлено в таблиці 1.1.

Таблиця 1.1

Порівняння протоколів IPSec і SSL

Технологія	IPSec	SSL
Апаратна залежність	Так	Так
Код	Не потребує змін для додатків. Може вимагати доступ до вихідного коду стека	Потрібні зміни в додатках. Можуть знадобитися нові DLL або доступ до вихідного коду додатків.
Захист	IP-пакет цілком. Включає захист для протоколів верхніх рівнів.	Тільки рівень додатків.
Фільтрація пакетів	Заснований на автентифікованих заголовках, адреси відправника і одержувача, і т.д. Проста і дешева, підходить для	Заснована на вмісті і семантиці високого рівня. Більш складна.
Платформи	Будь-які системи, включаючи	В основному, кінцеві системи (клієнти/сервери), а також
Firewall/VPN	Весь трафік захищений.	Захищений тільки трафік рівня додатків.
Прозорість	Для користувачів і додатків.	Тільки для користувачів.

Порівнюючи протоколи IPSec та SSL можна відмітити, що IPSec має більше переваг, ніж його конкурент та являється лідером у реалізації віртуальних приватних мережах.

Висновки:

Після аналізу в першому розділі, можна зробити висновок, що успішна робота підприємств, які використовують ті чи інші інформаційні системи, залежить від того наскільки добре вони захищені від можливих загроз безпеки. Якщо організація не може бути впевнена, що її конфіденційна інформація захищена від витоку або пошкодження, їй варто відмовитися від використання інфо-комунікаційних послуг, що в умовах сучасної економіки практично нереально, так як неминуче призведе до втрати можливості швидко реагувати на зміни ринку, а отже, до втрати конкурентоспроможності.

Отже, коли є необхідність працювати в інформаційному просторі і передавати дані через загальнодоступні мережі, такі як Інтернет, виникає гостра потреба у надійному захисті інформації. Це дозволяє стверджувати, що проблема захисту інформації сьогодні є важливою і актуальною.

Програмно-технічні засоби забезпечення інформаційної безпеки є основою системи захисту інформації. Це сукупність алгоритмів, програм і протоколів, що забезпечують шифрування, контроль за НСД, захист від шкідливих програм і багато іншого.

У роботі розглянуто два найбільш використовуваних протоколи захищеної передачі даних (як засоби забезпечення безпеки в Інтернеті) – SSL (TLS) та IPSec.

Протокол IPSec використовується в більшості реалізацій віртуальних приватних мереж. На сьогоднішній час на ринку представлені як програмні реалізації (наприклад, протокол реалізований в операційній системі IOS компанії Cisco), так і програмно-апаратні реалізації. Саме тому цей протокол буде детально розглянуто у 2 розділі [9,11].

РОЗДІЛ 2.
АНАЛІЗ НАБОРУ ПРОТОКОЛІВ IPSEC, ЯКІ ЗАБЕЗПЕЧУЮТЬ ЗАХИСТ ДАНИХ

2.1 Аналіз структури протоколів IPSec

Корпорація Cisco надає технологію IPSec, вбудовану в операційну систему IOS, яка дозволяє захищати мережу, як від зовнішніх, так і від можливих внутрішніх атак. IPSec (Internet Protocol Security) — система стандартів, спрямована на встановлення і підтримання захищеного каналу зв’язку для передачі даних. IPSec передбачає автентифікацію при встановленні каналу, шифрування переданих даних і поширення секретних ключів, необхідних для роботи протоколів автентифікації і шифрування. Засоби IPSec реалізують захист вмісту пакетів IP, а також захист від мережевих атак шляхом фільтрації пакетів та використання тільки надійних з’єднань. Систему відкритих стандартів Internet Protocol Security (IPSec) запропонувала Робоча група інженерів Інтернету (IETF). Протоколи IPSec забезпечують захист мереж, використовуючи для цього криптографічні протоколи безпеки і динамічне управління ключами.

Стек протоколів IPSec діє на мережевому рівні, захищаючи і автентифікуючи IP-пакети між пристроями, які беруть участь у з'єднанні. Він не прив'язаний до конкретних алгоритмів шифрування чи автентифікації або технології генерації ключів, може використовуватися для захисту одного або декількох «шляхів» між парою вузлів, між парою шлюзів безпеки або між шлюзом безпеки і вузлом [7].

Служби безпеки IPSec:

Конфіденційність – шифрування даних, що передаються з метою їх захисту від несанкціонованого перегляду.

Цілісність даних – гарантує, що дані в процесі передачі через Інтернет не були змінені. IPSec гарантує цілісність даних за допомогою контрольних сум, простої перевірки по надмірності.

Автентифікація – гарантує, що з'єднання встановлено з потрібним партнером. Одержувач може автентифікувати джерело пакета, гарантуючи і сертифікуючи справжність джерела інформації.

Захист від повторення пакетів (захист від replay-атак) – гарантує, що кожен пакет унікальний і не дублюється. Захист пакетів IPSec забезпечується за рахунок порівняння номерів послідовності отриманих пакетів зі плаваючим вікном хоста призначення або шлюзу безпеки. Пакет з номером послідовності нижче плаваючого вікна вважається таким що запізнився або дубльованим. Пакети що затримались або були дубльовані – відкидаються.

IPSec підтримує дві форми цілісності: цілісність, яка не залежить від з'єднання і часткову цілісність послідовності. Цілісність, яка не залежить від з'єднання, є сервісом безпеки, задача якого – визначити модифікацію конкретної IP датаграми.

IPSec використовує два протоколи для забезпечення безпеки трафіку Authentication Header (AH) і Encapsulating Security Payload (ESP), рис. 2.1 [7].

Рис. 2.1 Протоколи безпеки IPSec

Authentication Header (AH) забезпечує автентифікацію і цілісність IP-пакетів, що передаються між двома системами, і додатково може забезпечувати anti-replay

сервіс. AH не забезпечує конфіденційності (шифрування) пакетів. Дані передаються в незашифрованому вигляді. AH – це протокол, який слід використовувати, коли конфіденційність не потрібна або не дозволена.

Encapsulating Security Payload (ESP) протокол забезпечує конфіденційність (шифрування), цілісність і автентифікацію даних. Хоча використання шифрування і автентифікації в протоколі ESP необов'язково, необхідно вибрати хоча б одну з цих функцій. Так само ESP може додатково забезпечувати anti-replay сервіс.

Протокол IKE (Internet Key Exchange) використовується для визначення способу ініціалізації захищеного каналу, крім того, IKE визначає процедури обміну та управління секретними ключами з'єднання.

IPSec використовує сучасні алгоритми шифрування, автентифікації і обміну ключами. Деякі з стандартних алгоритмів, що використовуються в IPSec, перераховані нижче:

- DES: Виконує шифрування і розшифрування даних 56-бітним ключем.
- 3DES: Використовує 3 різних 56 бітних ключа (DES encrypt, DES decrypt, DES encrypt), пропонує значне збільшення криптографічної складності в порівнянні з 56-бітовим алгоритмом DES.
- AES: Забезпечує підвищену складність шифрування в залежності від використовуваної довжини ключа, використовує ключ 128 – 256 біт.
- MD5: автентифікує дані пакета з використанням 128-бітного загального секретного ключа.
- SHA-1: автентифікує дані пакета з використанням 160-бітного загального секретного ключа.
- DH: Для обміну секретними ключами в IPSec використовується алгоритм Diffie-Helman, що дозволяє двом сторонам формувати загальний секретний ключ, який використовується для алгоритмів шифрування і хешування по небезпечному каналу зв'язку.

IPSec надає структуру, адміністратор обирає алгоритми, на базі яких реалізуються служби безпеки в рамках цієї структури. На рис. 2.2 наведена структура IPSec.

Рис. 2.2 Структура IPSec

Протокол IPSec забезпечує сервіси безпеки на IP-рівні, обираючи потрібні протоколи безпеки, а також визначаючи алгоритми, що використовуються сервісами, надаючи криптографічні ключі для необхідних сервісів [7].

Загальний набір параметрів безпеки IPSec називається політикою. Політика складається з набору правил, що визначають обробку мережевого трафіку. Кожне правило містить набір фільтрів та дії, які це правило буде виконувати з пакетом, відповідно до умов фільтру. В якості параметрів фільтрів можуть бути задані IP-адреси, адреси мережі або повне доменне ім'я відправника і одержувача пакета, тип IP-протоколу (ICMP, TCP, UDP тощо), номери TCP і UDP портів відправника і одержувача.

Правило визначає, які методи автентифікації потрібні для обміну даними між хостами. У якості дії задається один з наступних параметрів – пакет блокується

(Block), передається без застосування IPSec (Permit) і передається із застосуванням IPSec (Security Association, узгодження безпеки).

Протокол IKE дозволяє встановити довірчі відносини між хостами, узгодити параметри безпеки і динамічного створення загального ключа. Угода про параметри безпеки, під управлінням яких створюється ключ, називають асоціацією безпеки (SA, security association). Протокол IKE, що включає ISAKMP і Oakley, використовує рамкову структуру ISAKMP для підтримки підмножини режимів обміну ключами Oakley [7].

Протокол управління ключами Асоціації безпеки Інтернет (Internet Security Association Key Management Protocol — ISAKMP) визначає процедури встановлення, погодження, зміни і видалення SA. Всі процеси узгодження параметрів проходять через ISAKMP, такі як authentication header та payload encapsulation. ISAKMP виконує автентифікацію, але не включає обмін ключами.

Задля створення ключів сесії Інтернет Oakley Key Determination Protocol (протокол визначення ключів) використовує гібридний метод Діффі-Хеллмана. Ці ключі створюються спеціально для центральних маршрутизаторів та комп’ютерів. Протокол Oakley вирішує важливе завдання забезпечення повної безпеки естафетної передачі даних. Він заснований на криптографічних методах. Повний захист естафетної передачі означає, що якщо навіть один ключ стане розкритий, то розкрито буде тільки ті дані, які зашифровані саме цим ключем. На рахунок даних, які були зашифровані наступними ключами, вони залишаться у повній безпеці [7].

Поняття асоціації безпеки SA є фундаментальним в IPSec. Її призначення — захистити процес обміну інформацією між двома сполученими сторонами. SA включає наступні дані, рис. 2.3:

- IP-адресу одержувача.
- Протокол безпеки, який використовується при передачі даних.
- Секретні ключі, що застосовуються при шифруванні.

– Метод форматування, який визначає, яким чином створюються заголовки і те, яка частина цих заголовків і даних користувача буде захищена в процесі передачі даних.
– Індекс параметрів захисту (Security Parameter Index — SPI) — один з ідентифікаторів SA. Він визначає те, як приймаюча сторона буде обробляти потік даних що надходить.

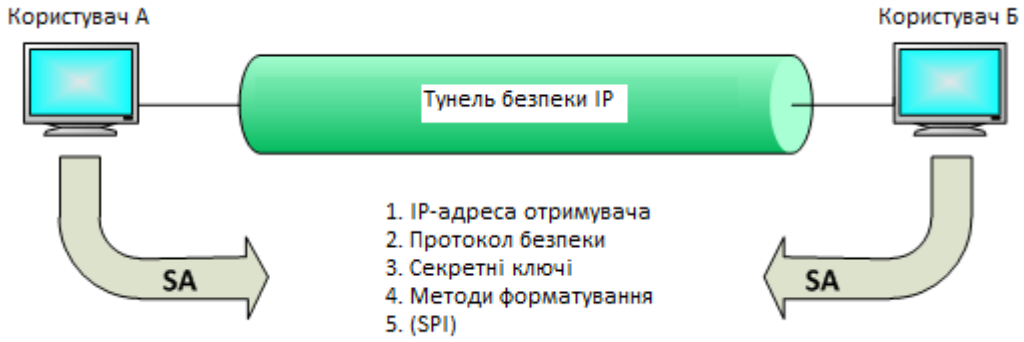

Рис. 2.3 Асоціація безпеки і тунель IP

SA – це сукупність параметрів з'єднання, які дають можливість сервісам забезпечувати захищений трафік. SA є односпрямованою, тобто визначає виконувані дії при передачі даних тільки в одному напрямку. Таким чином, при двонаправленому з'єднанні повинні використовуватися дві SA, по одній на кожен напрямок. Основною ідеєю двосторонньої передачі даних є використання двох SA з однаковими метахарактеристиками, але різними ключами. Ця ідея відома під назвою двонаправлених SA. SA можуть бути згруповані разом (пакет SA) для забезпечення необхідних властивостей захисту даних. SA визначає використання протоколів безпеки AH або ESP. Якщо до потоку трафіку застосовуються обидва протоколи, то для кожного з них створюється своя SA. Правилом для таких пакетів SA є однакова IP-адреса одержувача у всіх SA пакета [7].

SA однозначно визначається трійкою, що складається з Security Parameter Index (SPI), IP Destination Address (адреса призначення) і ідентифікатор протоколу безпеки (AH або ESP) [7].

Розглянемо типові для Інтернету асоціації безпеки, необхідні для роботи IPSec-сумісних вузлів і шлюзів безпеки:

Асоціація безпеки і відповідний їй тунель, що з'єднує два хости, забезпечуючи таким чином наскрізний захист переданих даних. В даному випадку Інтернет або Інтранет не має поняття про асоціації безпеки і не бере участі в ній, рис. 2.4.

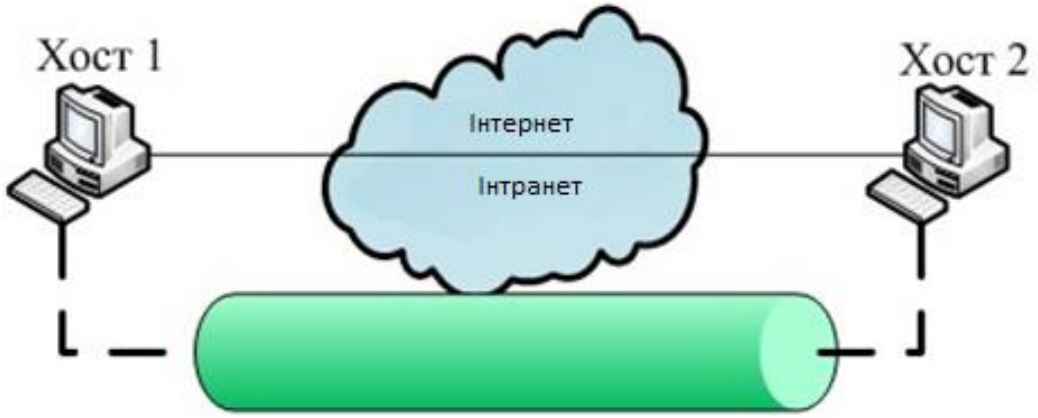

Рис. 2.4 Режим хост – хост

Асоціація безпеки і відповідний їй тунель розташовуються між двома шлюзами безпеки. Хости звільнені від необхідності застосування асоціації безпеки, і передбачається, що їх зв'язок зі шлюзами здійснюється за безпечним з'єднанням. В цьому випадку може використовуватися одна SA для обміну даними всередині, наприклад, групи суміжних підмереж, рис. 2.5.

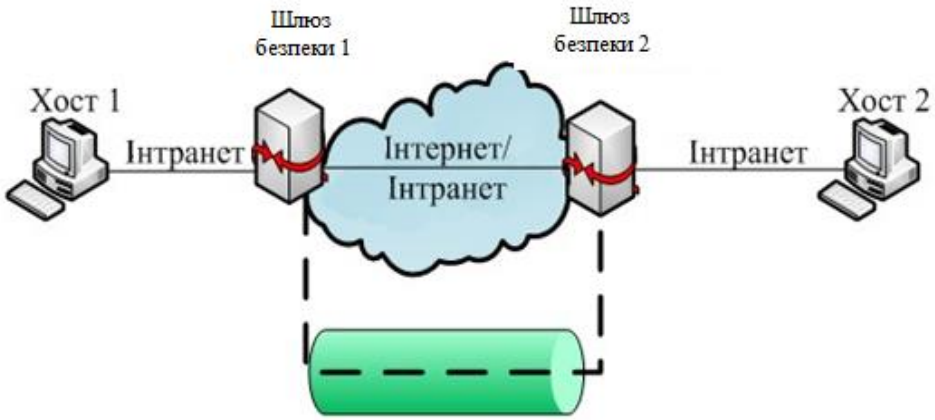

Рис. 2.5 Режим шлюз – шлюз

Тунель використовується як між шлюзами безпеки, так і для прямого зв'язку між хостами, рис. 2.6.

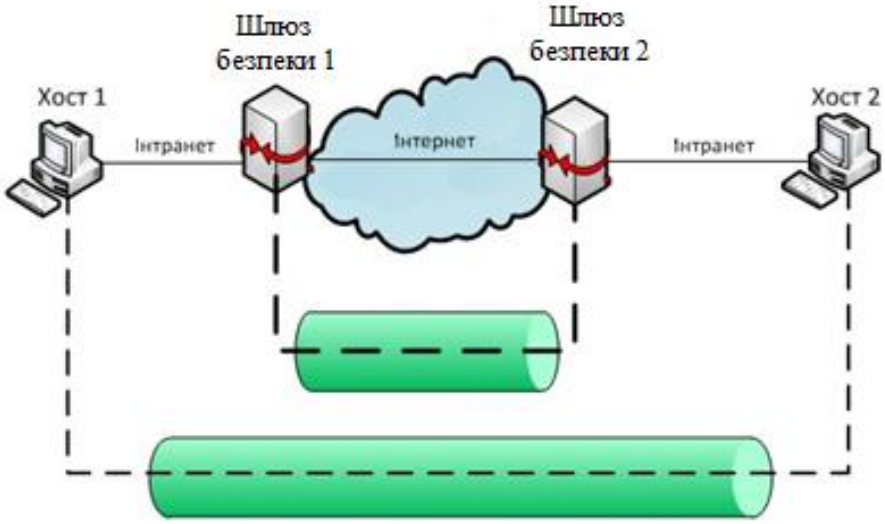

Рис. 2.6 Комбінований режим

Ситуація, коли віддалений хост (Хост 1) з'єднується з організацією через Інтернет або коли сервер знаходиться позаду шлюзу безпеки. З'єднання відбувається через Інтернет. Прикладом такого випадку можуть бути користувачі стільникових телефонів, рис. 2.7.

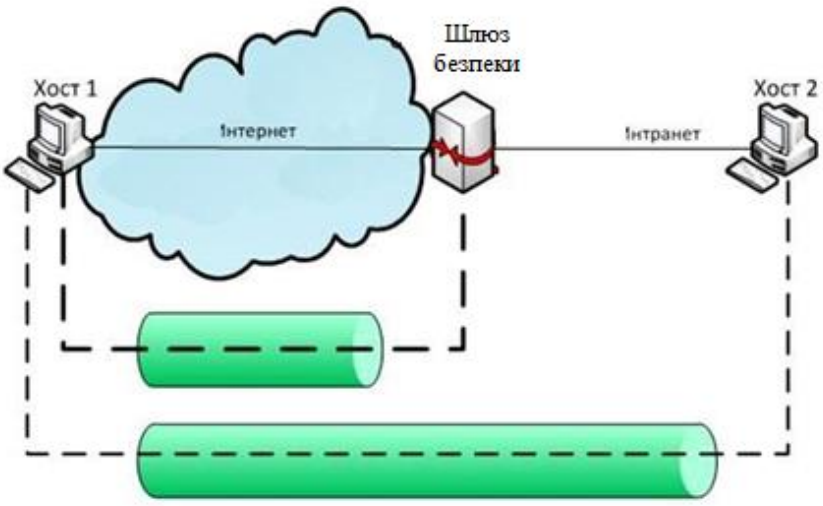

Рис. 2.7 Комбінований режим

Визначено два режими SA: режим транспорту і режим тунелювання. Режими роботи протоколів IPSec забезпечують різний рівень безпеки і застосовуються в різних умовах.

Транспортний режим забезпечує безпечне з'єднання між двома комп'ютерами, як правило, об'єднаними єдиною (локальної) мережею. При використанні транспортного режиму забезпечується захист поля корисних даних IP, що містить протоколи транспортного рівня (TCP, UDP), яке, в свою чергу, містить інформацію прикладних служб. Транспортний режим служить для захисту даних переважно всередині однієї мережі, безпека якої не може бути надійно забезпечена іншими способами без значних витрат, або коли вимагається високий рівень безпеки, що досягається спільним використанням різних протоколів. В якості прикладів можна назвати бездротові мережі, а також кабельні мережі, що покривають великі території.

- Транспортний режим є режимом для IPSec за замовчуванням.

Недоліком транспортного режиму є відсутність механізмів приховування конкретних IP-адрес відправника і одержувача пакета, а також можливість проведення аналізу трафіку. Результатом такого аналізу може стати інформація про обсяги і напрямки передачі інформації, сфера інтересів абонентів, розташування керівників [13].

- Режим тунелювання. Якщо хоча б одним з кінців з'єднання є шлюз безпеки, то SA обов'язково повинна виконуватися в тунельному режимі. Два хоста можуть при бажанні так само встановлювати режим тунелювання. Тунельний режим протоколу IPSec використовується в тих випадках, коли потрібно захистити дані (у тому числі заголовки IP), що передаються через загальнодоступну мережу. Прикладами можуть служити зв'язки між віддаленими підрозділами компанії [7].

Тунельний режим передбачає шифрування всього пакету, включаючи заголовок мережевого рівня. При використанні цього режиму весь пакет IP інкапсулюється в заголовок AH або ESP і додається додатковий заголовок IP. Заголовок протоколу безпеки розташований між зовнішнім і внутрішнім IP-

заголовком. IP-адреси зовнішнього заголовка вказують кінцеві точки тунелю, а IP-адреси інкапсульованого заголовка вказують вихідну точку і точку призначення пакета. Завдяки цьому забезпечується захист всього IP-пакета, включаючи заголовок IP [10,12].

При цьому, адресні поля зовнішнього заголовка мережевого рівня пакета, що використовує тунельний режим, заповнюються фаєрволом організації і не містять інформації про конкретного відправника пакета. При передачі інформації з зовнішнього світу в локальну мережу організації в якості адреси призначення використовується мережева адреса міжмережевого екрану. Після розшифровки міжмережевим екраном початкового заголовка мережевого рівня пакет направляється одержувачу [12,13].

На рис. 2.8, а) показана структура вихідного IP-пакета, на рис. 2.8, б) показаний пакет транспортного режиму, а на рис. 2.8, в) — тунельного. У разі використання ESP в пакетах з'являється два додаткових поля: ESP-кінцевик і значення MAC. MAC – це код ідентифікації повідомлення, для якого використовується значення перевірки цілісності ICV, для чого IPSec вимагає реалізації процедур HMAC-MD5 і HMAC-SHA-1. Ці поля поміщаються після поля L_7, яке являє обмін даними протоколів прикладного рівня (FTP, HTTP та ін).

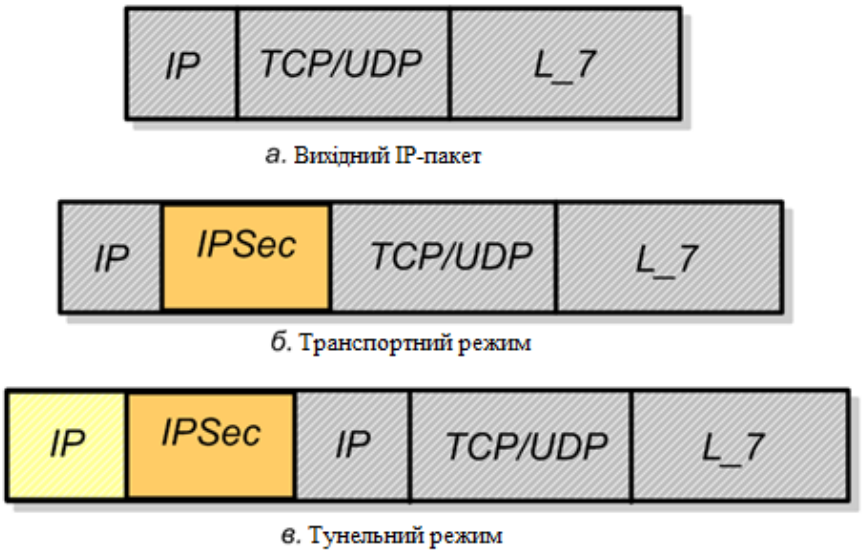

Рис. 2.8 Структура IP-пакету в різних режимах

IPSec потребує у великій кількості інформації для забезпечення безпеки користувачів. SA визначає, які послуги по забезпеченню захисту надаються користувачеві. Такі вимоги до безпеки зберігаються в двох базах даних: БД асоціацій безпеки (SAD) і БД Політики Безпеки (SPD). Вони є сховищами інформації для IPSec, а їх вміст, що конфігурується адміністратором безпеки, керує «поведінкою» IPSec. SAD містить параметри, які пов'язані з кожною активною асоціацією безпеки. Оскільки SA є односпрямованими, в SAD зберігаються пари SA, по одній для кожного напряму.

В базі даних SAD міститься [14]:

– AH: алгоритм автентифікації,
– AH: автентифікаційний секретний ключ (authentication secret),
– ESP: алгоритм шифрування,
– ESP: секретний ключ шифрування,
– ESP: дозвіл автентифікації (yes/no),
– Параметри обміну ключами,
– Обмеження маршрутизації,
– IP політика фільтрації.

SPD описує політики, які визначають характер обробки всього IP-трафіку, тобто задають, який потік даних і яким чином цей потік даних обробляється (відкинути, обійти IPSec, застосувати IPSec), як обробляти вхідні і вихідні потоки. Таким чином, до цієї бази даних звертаються для обробки кожного вхідного і вихідного пакету. Кожен запис в SPD визначається набором значень полів IP і протоколу верхнього рівня, званих селекторами. Ці селектори використовуються для фільтрації вихідного трафіку, для того щоб поставити його у відповідність з певною SA. Обробка вихідних IP-пакетів здійснюється в наступній послідовності [14]:

– Порівнюються значення відповідних полів у пакеті (селекторні поля) з SPD і знаходиться нуль або більше SA.
– Визначається SA (якщо така є) для пакета і пов'язаний з нею SPI.

– Виконуються необхідні операції IPSec (AH або ESP).

– SPD запис визначається наступними селекторами:

– IP-адреса місця призначення.

– IP-адреса відправника.

– UserID – ідентифікатор користувача, служить для ідентифікації політики, відповідно до ім’я користувача або системи.

– Рівень чутливості даних.

Протокол транспортного рівня. Це значення береться з поля «наступний заголовок» пакета IPv4 або IPv6. Це може бути індивідуальний код протоколу, список кодів протоколу або діапазон таких кодів.

Протокол IPSec (AH, ESP або AH/ESP). Витягується (якщо є) з поля «наступний заголовок» пакета IPv4 або IPv6.

Порти відправника і одержувача. Це можуть бути індивідуальні номери портів TCP або UDP, список портів або довільний порт.

Клас IPv6. Значення класу виходить з заголовка IPv6. Це може бути специфічне значення і код довільного класу.

Мітка потоку IPv6. Значення мітки потоку виходить із заголовка IPv6. Це може бути специфічне значення мітки потоку або код довільній мітки.

Тип сервісу IPv4. Значення ToS виходить із заголовка IPv4. Це може бути специфічне значення ToS або покажчик довільного значення.

Кожен мережевий інтерфейс, для якого необхідна обробка IPSec, вимагає визначення баз даних для вхідного і вихідного трафіку [7].

2.2 Принцип роботи протоколів IPSec

Протокол IPSec складається з трьох основних компонентів: служби агента політики IPSec, обміну ключами в Інтернеті (IKE), а також драйвера IPSec [15].

Етапи роботи IPSec:

Початок процесу IPSec. Додаток, трафік якого вимагає захист IPSec, починає процес обміну даними IKE-протоколу.

Перша фаза IKE. Головною метою обміну даними, що відбувається в першій фазі IKE, є автентифікація сторін IPSec і створення захищеного каналу між сторонами, що дозволяє почати обмін IKE. Основним результатом цієї фази є узгодження параметрів асоціацій захисту IKE (SA) між сторонами з метою створення захищеного каналу для наступних обмінів IKE.

Друга фаза IKE. IKE-процес веде узгодження параметрів асоціації безпеки IPSec, встановлює відповідні асоціації безпеки IPSec з метою створення тунелю IPSec. Передача даних. Відбувається обмін даними між сполученими сторонами IPSec, який ґрунтується на параметрах IPSec і ключі, що зберігаються в базі даних асоціацій безпеки [17].

Завершення роботи IPSec. Асоціації безпеки IPSec завершують свою роботу або в результаті їх видалення, або через перевищення граничного часу їх існування [17].

Як відбувається обмін даними між двома хостами з застосуванням IPSec, показано на рис. 2.9.

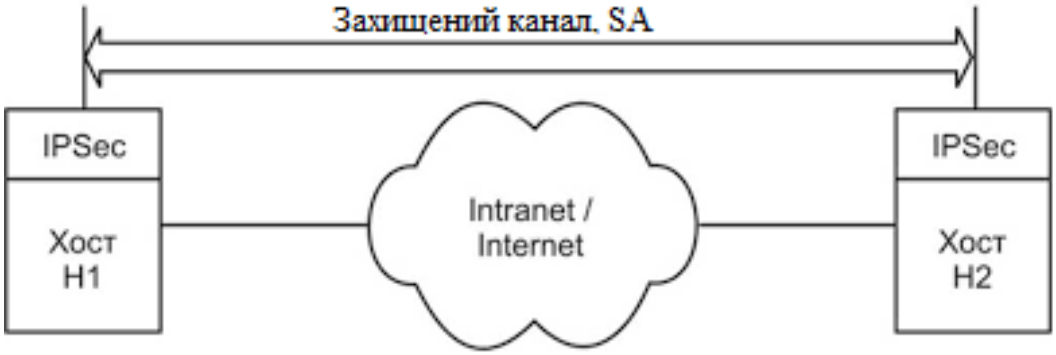

Рис. 2.9 Обмін даними між двома хостами із застосуванням IPSec

Обмін ключами в Інтернеті. Перед початком безпечного обміну даними між двома комп'ютерами повинно бути встановлено безпечне підключення. Для створення угоди між двома комп'ютерами існує метод зіставлення безпеки і дозволу

обміну ключами, який називається обміном ключами в Інтернеті (Internet Key Exchange, IKE). Даний метод централізує управління зіставлення безпеки, тим самим скорочуючи час підключення, а також створює загальні секретні ключі, які використовуються для захисту і управління даними [15].

Для забезпечення успішного та безпечного зв'язку, IKE виконує операцію в два етапи. На першому етапі (перша фаза IKE) два комп'ютери створюють безпечний канал з перевіркою автентичності, який називається зіставленням безпечного режиму. Під час цього етапу спочатку виконується узгодження політики безпеки основного режиму за допомогою алгоритму шифрування (DES або 3DES), алгоритму перевірки цілісності (MD5 або SHA1), групи Діффі-Хеллмана або методу автентифікації Kerberos, сертифікат або ключ). Після цього на першому етапі здійснюється обмін відомостями, які необхідні алгоритму визначення ключа Діффі-Хеллмана для створення загального секретного ключа. Після обміну на кожному комп'ютері створюється основний ключ, використовуваний для захисту автентифікації [15-**Ошибка! Источник ссылки не найден.**].

Останнім кроком на цьому етапі є перевірка достовірності. У цей момент комп'ютери виконують автентифікація при обміні ключами Діффі-Хеллмана. Всі відомості облікового запису хешуються і шифруються за допомогою ключів, створених за результатами обміну відомостями про групу Діффі-Хеллмана на попередньому кроці [**Ошибка! Источник ссылки не найден.**].

Асоціація безпеки IKE визначає параметри обміну IKE: використовуваний метод автентифікації, алгоритми шифрування і хешування, використовувана група Діффі-Хеллмана, максимальний час існування асоціації захисту IKE в секундах або кілобайтах і спільно використовувані секретні значення ключів для шифрування [18]. Таким чином, в ході першої фази IKE виконуються наступні дії, рис. 2.10:

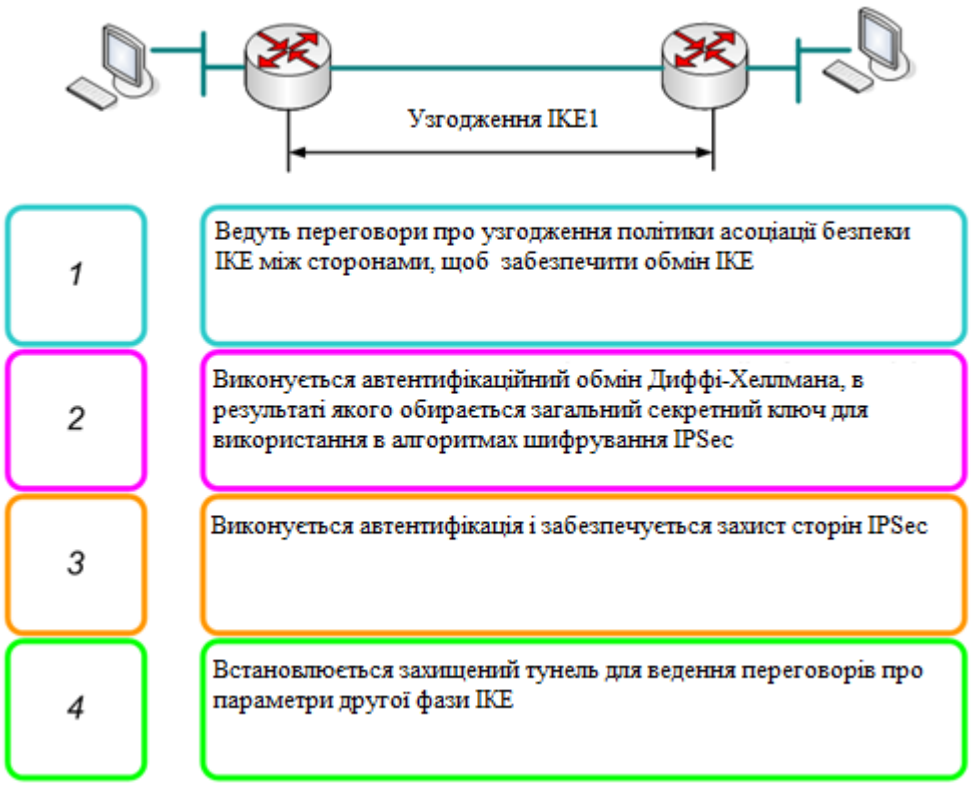

Рис. 2.10 1 фаза IKE

Перша фаза IKE може виконуватися в одному з двох режимів: основному (Main Mode) і агресивному (Aggressive Mode). В агресивному режимі менша кількість обмінів параметрами між сторонами, і як наслідок, менша кількість пакетів пересилаються, в результаті чого необхідно менше часу для встановлення сеансу IPSec. Однак, недоліком використання агресивного режиму є те, що обидві сторони обмінюються інформацією до того, як створений захищений канал.

На другому етапі обміну ключами в Інтернеті (друга фаза IKE) зіставлення безпеки узгоджуються від імені драйвера IPSec. Друга фаза IKE виконується в швидкому режимі, після того як в результаті першої фази IKE створюється захищений тунель. Під час цього етапу виконуються наступні кроки: йде узгодження політики, під час якого драйвери IPSec обмінюються такими вимогами до захисту передачі даних, як режим AH або ESP, алгоритм хешування для автентифікації (MD5 або SHA1), а також, якщо запитується, алгоритм шифрування (DES, 3DES, AES). Далі відбувається оновлення або обмін матеріалом для створення

ключа сеансу. В цей час IKE оновлює відомості про ключі, після чого відбувається створення нових загальних ключів для автентифікації і шифрування пакетів. І, наостанок, йде процес зіставлення безпеки, після чого ключі передаються в драйвер IPSec разом з SPI [15-**Ошибка! Источник ссылки не найден.**,19].

Таким чином, завданням другої фази IKE є узгодження параметрів асоціації безпеки IPSec з метою створення тунелю IPSec. У цій фазі виконуються наступні дії, рис. 2.11.

Драйвер IPSec отримує список активних фільтрів від агента політики IPSec і після чого звіряє всі вхідні і вихідні пакети з фільтрами в поточному списку. У тому випадку, якщо пакет повністю співпадає з даним фільтром, то до нього застосовується дія самого фільтра. Якщо ж пакет не відповідає ні одному доступному фільтру, то він повертається в драйвер TCP/IP для прийому або передачі без всяких змін. Як для обробки вхідного, так і вихідного трафіку застосовуються ключі і зіставлення безпеки швидкого режиму. У свою чергу, драйвер IPSec містить у своїй базі даних всі поточні співставлення безпеки швидкого режиму і для правильного застосування зіставлень безпеки і пакетів використовує індекс параметрів безпеки [15].

Рис. 2.11 2 фаза IKE

Після того, як узгодження безпеки буде завершено, драйвер IPSec приймає від IKE зіставлення безпеки, яке містить ключ сеансу. Потім драйвер IPSec в базі даних знаходить зіставлення безпеки і вставляє індекс параметрів безпеки в заголовок AH або ESP. Після цього він підписує пакети і відправляє їх на рівень IP для пересилання на комп'ютер призначення [15].

Після завершення другої фази IKE і створення асоціацій захисту IPSec в швидкому режимі, починається обмін інформацією через тунель IPSec. Пакети шифруються і розшифровуються за допомогою алгоритмів шифрування та ключів, зазначених асоціацією захисту IPSec [19].

При отриманні IP-пакетів, які вважаються небезпечними, драйвер IPSec завжди їх звіряє зі списком фільтрів передачі даних між сторонами підключення.

Асоціація безпеки IPSec задає також межу часу свого існування в кілобайтах переданих даних або в секундах. Вона має спеціальний лічильник, значення якого зменшується на одиницю за кожну секунду або після передачі кожного кілобайта даних [18-19].

По закінченні передачі всіх даних узгодження швидкого режиму видаляються, однак зіставлення основного режиму залишається чинним якийсь час. Цей інтервал (час життя) задається в настройках IPSec – політики. Він дозволяє при поновленні передачі даних виконувати лише узгодження швидкого режиму, економлячи час, необхідний для встановлення захищеного з'єднання.

Переваги та недоліки використання IPSec. IPSec зазвичай застосовується для створення VPN-тунелів між комп'ютерами або мережами через Інтернет, або іншу масштабну мережу, безпеку якої неможливо контролювати, і є найбільш визнаним, підтримуваним і стандартизованим з усіх протоколів віртуальних приватних мереж (ВПМ, VPN). Для забезпечення спільної роботи різних пристроїв у гетерогенній мережі він підходить краще інших, так як заснований на повністю відкритих стандартах. На відміну від інших VPN-протоколів, IPSec працює на третьому рівні і може захищати будь-який IP-трафік. При його застосуванні з іншими протоколами тунелювання на другому рівні, такими як L2TP, також з'являється можливість захисту і не IP-трафіку.

IPSec – це не жорсткий протокол, який диктує тип алгоритму, ключів і використовуваних методів автентифікації. IPSec – це відкрита модульна платформа, що забезпечує більшу гнучкість для компаній, що вибрали цю технологію. Великою перевагою IPSec залишається те, що він працює на будь-якому виробнику, що підтримує IPSec RFC, отже, використання IPSec вирішує проблеми сумісності. Те, що IPSec є відкритим стандартом і працює на третьому рівні, дозволяє йому вирішувати більш складні завдання.

Одною з важливих переваг IPSec є невисока вартість його використання, оскільки він дозволяє захистити дані та забезпечити перевірку автентичності користувачів і даних без додаткових затрат на мережеве обладнання, так як зберігається сумісність зі всім раніше випущеними обладнанням, а також те, що протокол є стандартним і відкритим, і поставляється практично з усіма сучасними операційними системами.

IPSec забезпечує високий рівень безпеки за допомогою служб, заснованих на криптографії (хешування – для захисту від повторень, забезпечення цілісності даних і перевірки їх достовірності (перевірки прав доступу), і безпосередньо шифрування, що забезпечує конфіденційність даних).

Важливою перевагою IPSec, є простота використання IPSec. Для використання IPSec потрібно лише налаштувати і запустити політику безпеки IPSec. IPSec прозорий для кінцевих користувачів і додатків. Протокол IPSec інтегрований на мережевому рівні, забезпечує безпеку для всіх протоколів, заснованих на IP, пакетах TCP/IP, а значить, при реалізації IPSec брандмауера або маршрутизатора немає необхідності вносити зміни в мережеві додатки настільного ПК, а також немає необхідності перенавчати кінцевих користувачів. Так само при використанні IPSec існує можливість централізованого управління політикою IPSec. IPSec можна налаштовувати через групову політику, політику IP-безпеки або за допомогою правил безпеки підключень. Дана можливість дозволяє застосовувати політики IPSec на домен, сайт або певний підрозділ, усуваючи адміністративні витрати на налаштування кожного окремого комп'ютера.

За допомогою політики IPSec можна налаштувати сервер тільки на прийом трафіку певного типу. IPSec використовує методологію для фільтрації пакетів по IP, діапазонам IP – адрес, протоколам IP і певним TCP і UDP портам.

Політики IPSec можна створювати і налаштовувати відповідно до вимог безпеки додатків, комп'ютерів, груп комп'ютерів домену сайту або глобальної організації. IPSec можна налаштовувати для використання широкого спектру сценаріїв, включаючи пакетну фільтрацію, захист вузла трафіку хоста за вказаним шляхом, захист трафіку на сервери, тунельного протоколу рівня 2 (Layer Two Tunneling Protocol, L2TP), віртуальної приватної мережі (Virtual Private Network, VPN) і багато іншого.

В даний час не існує таких мережевих технологій, стандартів та алгоритмів, які були б повністю захищені і не вразливі для атак. Але, тим не менш, з розвитком інформаційних технологій способи захисту інформації стають все більш і більш досконалими. Раніше при передачі інформації по мережах можна було з допомогою нескладних дій перехоплювати пакети даних і отримувати доступ до їх вмісту, використовуючи легкий сніфер.

Зараз, при передачі даних застосовується шифрування, яке дозволяє захищати передану інформацію. Однак, на думку служб інформаційної безпеки, вся робота по захисту даних зводиться до мінімізації ризиків її витоку і не забезпечує повної її недоторканності.

Стандарт IPSec, як окремий і досить розповсюджений спосіб захисту інформації, так само, передусім призначений для мінімізації ризику розкриття трафіку при його перехопленні, тому при передачі інформації трафік шифрується. Головною ознакою стандарту IPSec, є handshake (привітання, рукостискання) обох хостів, за допомогою якого виявляється рівень довіри між ними [20].

2.3 Захист IP-пакетів з допомогою AH та ESP

У IPSec визначені два протоколи забезпечення безпеки AH і ESP.

Протокол AH (Authentication Header – заголовок автентифікації). Протокол захисту, що забезпечує автентифікацію (посвідчення походження даних або перевірку справжності), цілісність і, якщо це визначено асоціацією безпеки, захист від атак відтворення. Протокол AH діє як цифровий підпис і може гарантувати, що дані в пакеті IP неправомірно змінені не будуть, тобто протокол забезпечує цілісність, незалежну від з'єднання (connectionless integrity). Протокол AH не забезпечує сервіс шифрування і розшифрування, тому дані залишаються доступними для читання. AH підписує пакети використовуючи алгоритми хешування з ключами (MD5, а в більш сучасних реалізаціях SHA1) [19].

Протокол ESP (Encapsulating Security Payload – вкладені захищені дані). Протокол захисту, що забезпечує конфіденційність (шифрування), автентифікацію і цілісність даних, не залежну від з'єднання, а також, в якості опції, сервіс захисту від атак відтворення. У ESP автентифікація і цілісність, незалежна від з'єднання, що є пов'язаними операціями і називаються ідентифікацією. Вони пропонуються як необов'язкове доповнення до операцій шифрування. ESP може виконувати шифрування окремо від інших операцій, але таке відділення від операцій із забезпечення захисту даних і їх ідентифікації може призвести до атак на передані дані. Захист від повторення доступний лише у випадку, коли використовується автентифікація, та її застосування визначає одержувач. Конфіденційність потоку даних забезпечується тільки при використанні тунельного режиму.

Обидва протоколи є засобами контролю доступу і можуть застосовуватися як окремо, так і разом. Ці протоколи підтримують IPv4 і IPv6. Формати заголовків представлені на рис. 2.12 і рис. 2.13.

<table>
<tr><td>4
Версія
(Version)</td><td>4
Довжина заголовка
(Header Length)</td><td>8
Тип сервіса
(Type of Service)</td><td colspan="2">16
Загальна довжина пакета (Total Length)</td></tr>
<tr><td colspan="3">16
Загальний ідентифікатор
(Identification)</td><td>3
Прапор
(Flag)</td><td>13
Фрагментне зміщення
(Fragment Offset)</td></tr>
<tr><td colspan="5">IP-адреса відправника
(Source Address)</td></tr>
<tr><td colspan="5">IP-адреса отримувача

(Destination Address)</td></tr>
<tr><td colspan="3">Додаткові параметри IP

(Options)</td><td colspan="2">Заповнювач

(Padding, доповнює до 32 біт)</td></tr>
</table>

Рис. 2.12 Формат заголовку IPv4

<table>
<tr><td>4
Версія
(Version)</td><td>8
Клас трафіка
(Traffic Class)</td><td colspan="3">20
Мітка потока
(Flow Label)</td></tr>
<tr><td colspan="3">16
Довжина корисного навантаження (Payload Length)</td><td>8

Наступний заголовок
(Next Header)</td><td>8

Межа переходів
(Hop Limit)</td></tr>
<tr><td colspan="5">128
Адреса відправника
(Source Address)</td></tr>
<tr><td colspan="5">128
Адреса призначення
(Destination Address)</td></tr>
</table>

Рис. 2.13 Формат заголовку IPv6

Якщо значення поля може бути змінене в процесі передачі, то при обчисленні значення перевірки цілісності ICV значення цього поля прирівнюється до нуля. Якщо поле змінюється, але його значення у одержувача може бути передбачене, тоді це значення присвоюється з тим, щоб можна було порахувати ICV.

RFC 4302 є останньою специфікацією протоколу AH. На рис. 2.14 представлений формат цього варіанту протоколу. При використанні AH, протокольний заголовок (IPv4, IPv6), що безпосередньо передує заголовку AH, слід поміщати значення 51 в поле Protocol (IPv4) або Next Header (IPv6).

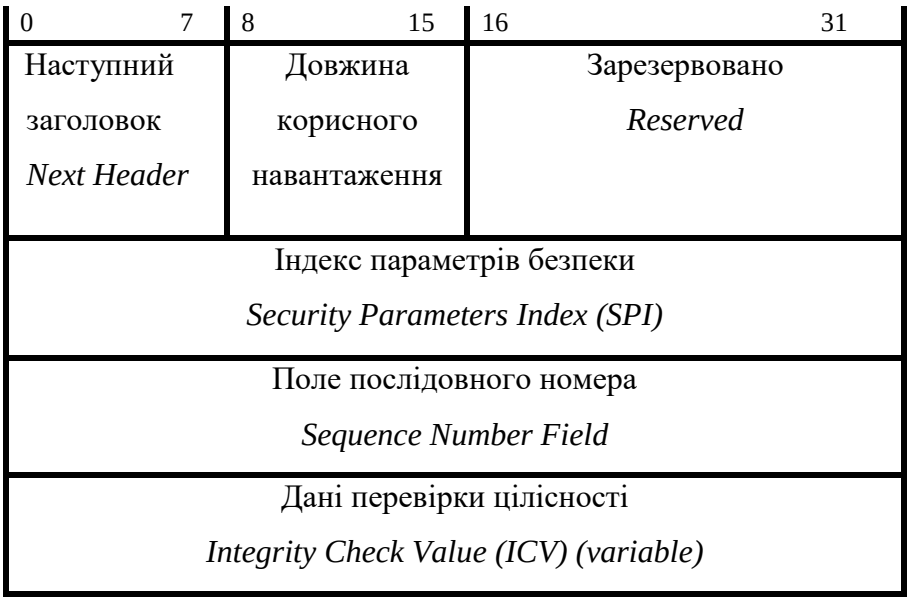

Рис. 2.14 Формат заголовку AH

Всі поля включаються в значення перевірки цілісності. Ці поля призначені для виконання наступних функцій:

– Наступний заголовок (Next Header). Поле, яке вказує тип даних, які передаються, виконуються після даних ідентифікації.

– Довжина переданих даних. Поле, яке вказує заголовок AH в 32 – бітових словах.

– Зарезервовано. Поле, яке є зарезервованим для майбутнього використання і повинно дорівнювати 0.

– Індекс параметра безпеки. Поле, значення якого в комбінації з IP-адресою одержувача та протоколом безпеки (AH), однозначно задає асоціації безпеки для даної дейтаграми. Якщо значення поля дорівнює нулю, це означає, що асоціації безпеки не існує.

– Поле послідовного номера. Значення поля послідовного номера формується відправником за замовчуванням і служить для захисту від replay – атак. Це поле завжди є, навіть якщо одержувач не використовує захист від повторень в даній SA. Якщо такий захист використовується, переданий послідовний номер не може повторюватися. Перший пакет асоціації безпеки має порядковий номер 1. Коли порядковий номер досягає максимального значення (4,294,967,295 або 2^{32}-1), нові зіставлення безпеки IPSec встановлюються для підтримання порядкового номера від повтору SA. Якщо ж встановлюються нові зіставлення безпеки IPSec, то порядковий номер для зіставлення безпеки починається з 0 [15].

– Дані ідентифікації. Поле змінної довжини, що містить значення перевірки цілісності ICV розрахунку відправника, тобто значення HMAC MD5 або HMAC SHA1.

Значення перевірки цілісності (Integrity Check Value — ICV) в AH обчислюються на основі:

– полів IP-заголовка, які або незмінні, або їх значення можна передбачити отримання;

– заголовка AH (а також можливих заповнюють бітів);

– всіх заголовків і даних верхнього рівня.

IP-пакет, до якого був застосований AH, може бути фрагментований маршрутизаторами на шляху від відправника до одержувача, але такі фрагменти повинні бути зібрані в ціле до обробки AH у одержувача. Вузол одержувача обчислює ICV на основі відповідних полів пакету і порівнює результат із значенням, переданим в поле «Дані Ідентифікації». Якщо вони збігаються, дейтаграма пропускається.

RFC 4303 – це остання специфікація ESP. Протоколу ESP організація IANA призначила номер 50. ESP складається з нешифрованого заголовка, за яким слідують зашифровані дані. Ці дані складаються з захищених полів заголовку ESP і даних користувача, якими може бути вся дейтаграма IP, включаючи заголовки верхнього рівня і дані користувача. На рис. 2.15 показаний формат заголовка ESP.

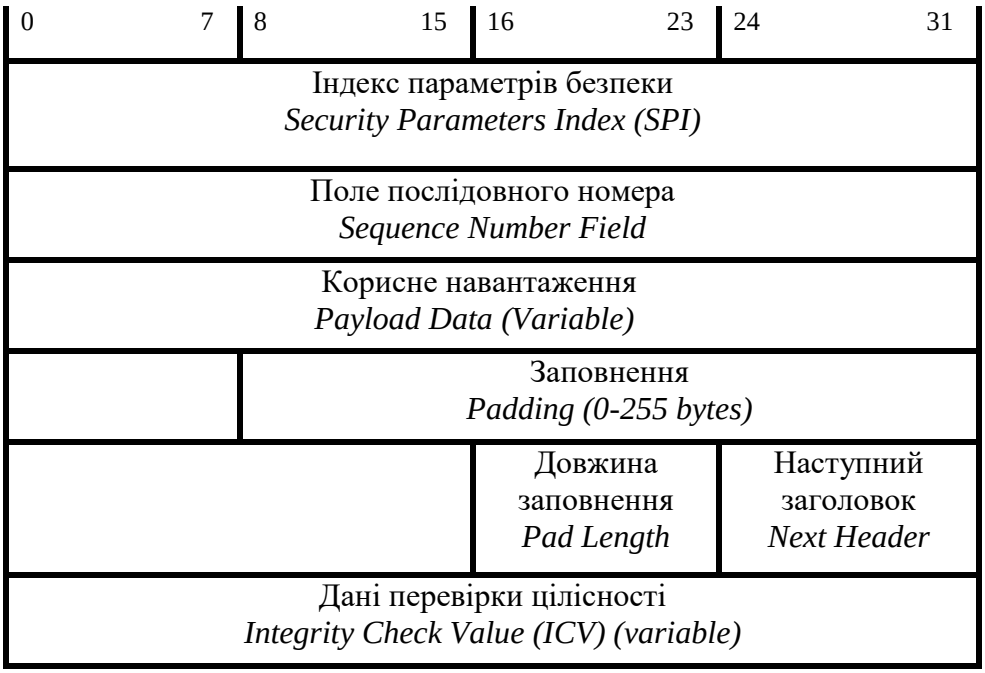

Рис. 2.15 Формат заголовку ESP

Всі поля повинні бути присутніми, і включаються до значення перевірки цілісності. Ці поля виконують наступні функції [15]:

– Індекс параметра безпеки. Значення цього поля, в комбінації з IP – адресою одержувача та номером протоколу (ESP), однозначно визначають асоціацію безпеки даної дейтаграми. SPI вибирається вузлом одержувача у процесі визначення SA.

– Послідовний номер. Як і в AH, ESP це поле завжди є, навіть якщо одержувач не збирається скористатися захистом від повторення в конкретному SA. Якщо ж такий захист застосовується (за замовчуванням це так), що послідовний номер не може повторюватися.

– Дані що передаються. Поле містить зашифровані дані.

– Додаток. Поле змінної довжини (від 0 до 255 байт), яке використовується для заповнення корисних даних відповідної довжини, служить для забезпечення вимоги про довжину відкритого тексту. Кількість доповнюючих байтів залежить від реалізації.

– Довжина доповнення. Поле довжиною в один байт, яке визначає кількість байтів в полі заповнення.

– Наступний заголовок. Однобайтове поле, яке використовується для визначення типу даних, що знаходяться в полі Передані дані.

– Перевірка достовірності даних. Поле змінної довжини, що містить значення ICV відправника, тобто значення HMAC MD5 або HMAC SHA1.

Обробка вихідних пакетів. Відправник при шифрування пакетів виробляє наступні дії:

– Поміщає в поле «Передані дані» ESP вихідну інформацію протоколу верхнього рівня, якщо перебуває в транспортному режимі, або всю вихідну датаграму IP, якщо перебуває в тунельному режимі.

– Доповнює до потрібної довжини, якщо необхідно.

– Шифрує результат (дані, що доповнюють біти, довжину доповнення і наступний заголовок) з використанням ключа алгоритму шифрування і режиму автентифікації, заданого в SA.

– Якщо вибрана ідентифікація, то спочатку виконується шифрування, яке не виконується над полем «Дані ідентифікації».

Обробка вхідних пакетів.

Якщо пакет, що прийшов на обробку ESP, є фрагментом, тобто поле зміщення фрагмента не дорівнює нулю чи встановлений прапор, який вказує, що повинні прийти ще фрагменти, то тоді одержувач повинен відкинути такий пакет і повідомити про помилку. Запис про це повинна містити значення SPI, дату та час отримання, адресу відправника, адресу отримувача, послідовний номер та (у разі IPv6) ідентифікатор потоку.

Пошук асоціації безпеки. По отриманні (зібраного) пакета, що містить заголовок ESP, одержувач визначає відповідну (двонаправлену) SA, ґрунтуючись на адресі одержувача, номер протоколу безпеки (ESP) і SPI. В SA повинно бути перевірено поле з послідовним номером, повинно бути присутнє поле ідентифікації і який алгоритм і ключі використовуються при розшифруванні і обчисленні ICV (якщо така обробка задана).

Перевірка послідовного номера. Всі реалізації ESP повинні забезпечувати захист від повторень, хоча такий захист може, в залежності від налаштувань в SA, і не використовуватися одержувачем.

Перевірка значення перевірки цілісності (ICV). Якщо в SA потрібне використання ідентифікації, то одержувач обчислює ICV для пакета ESP (за винятком поля з даними ідентифікації) із застосуванням зазначеного алгоритму ідентифікації та засвідчується, що отримане значення збігається з тим, що знаходиться в полі ідентифікації даного пакету. Якщо знову обчислене і передане ICV збігаються, то перевірка для даної дейтаграми вважається пройденою. Якщо ж вони не збігаються, то тоді одержувач повинен відкинути IP-пакет і повідомити про помилку.

Розшифрування пакета. Вузол IPSec виконує наступні дії:

– Розшифровує поля з блоком даних, які доповнюють бітами, довжиною доповнення і наступним заголовком з використанням ключа алгоритму розшифрування, режиму автентифікації і даними криптографічної синхронізації (якщо є), заданими в SA.

– Обробляє всі доповнюючі біти, як зазначено в специфікації алгоритму розшифрування.

Відновлює вихідну датаграму IP:

– Транспортний режим. З вихідного IP-заголовка та інформації вихідного протоколу верхнього рівня, що знаходиться в полі переданих даних ESP.

– Тунельний режим. З IP-заголовка і всієї дейтаграми IP, що знаходиться в полі переданих даних ESP.

Принцип роботи протоколу АН у транспортному та тунельному режимі:

Протокол АН може працювати в двох режимах — транспортний і тунельний. У транспортному режимі АН поміщається між заголовком IP і заголовком протоколу наступного рівня, як показано на рис. 2.16. У разі використання IPv4 заголовок АН вставляється після IP-заголовка і будь-яких налаштувань, і перед протоколом верхнього рівня (Upper-Level Protocol — ULP) або перед будь-яким іншим заголовком IPSec. «Протокол верхнього рівня» означає будь-який протокол, що використовує IP-датаграму. Такими протоколами можуть бути TCP, UDP, OSPF, ICMP і т. д.

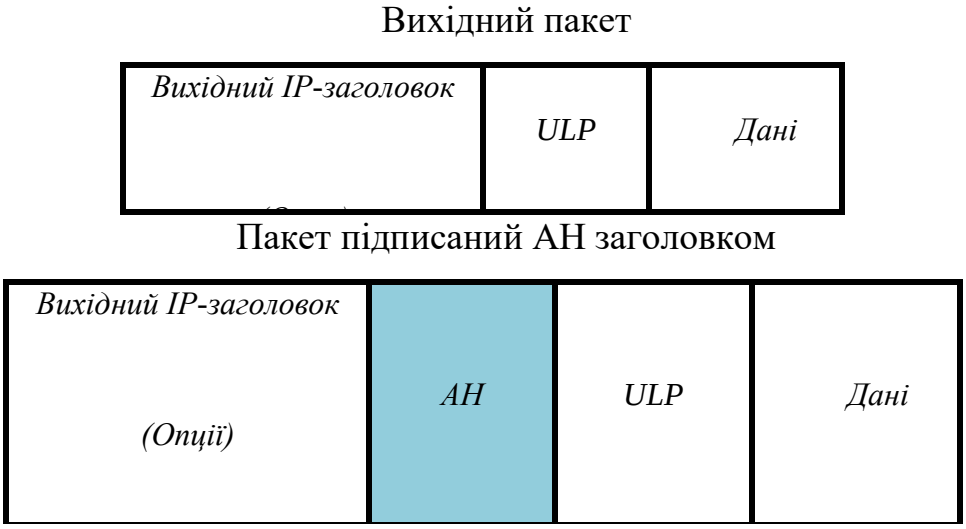

Рис. 2.16 Формат заголовку АН з IPv4

У разі використання IPv6 заголовок АН представляється як передані дані і розміщується після заголовків розміщення (hop-by – hop, routing, fragmentation). Заголовок (заголовки) розширень з налаштуваннями одержувача можуть з'явитися або перед, або після заголовка АН, в залежності від вимог. На рис. 2.17 показано розміщення АН для транспортного режиму у разі IPv6.

Вихідний пакет

Вихідний IP-заголовок	*Додаткові заголовки*	*ULP*	*Дані*

Пакет підписаний AH заголовком

Вихідний IP-заголовок (Опції)	*Пересилка, фрагментація, маршрутизація до отримувача*	*AH*	*Налаштування отримувача**	*ULP*	*Дані*

Рис. 2.17 Формат заголовку AH з IPv6

На рис. 2.18 і рис. 2.19 показаний захист AH у разі IPv4 і IPv6 в тунельному режимі. AH в режимі тунелювання підписує пакет для збереження цілісності та інкапсулює його в заголовки IP і AH, дані залишаються доступними для читання. При використанні протоколу AH в тунельному режимі, частини зовнішнього IP заголовка є захищеними так само, як і весь IP пакет що тунелюється, включаючи весь внутрішній IP-заголовок. У внутрішньому і зовнішньому заголовках можуть використовуватися різні версії IP (наприклад, IPv6 через тунель IPv4 або IPv4 через тунель IPv6) [7].

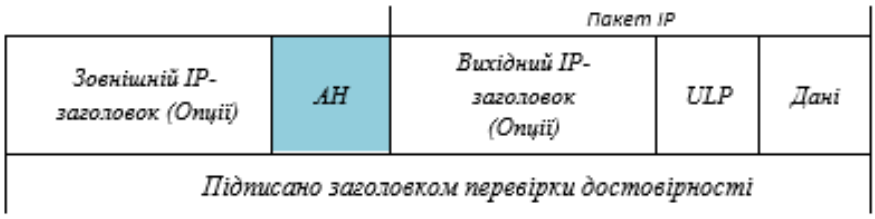

Рис. 2.18 Формат заголовку AH з IPv4

Рис. 2.19 Формат заголовку AH з IPv6

Принцип роботи протоколу ESP у транспортному та тунельному режимі:

Так само як і AH, протокол ESP може бути використаний у двох режимах: транспортний і тунельний. Протокол ESP в транспортному режимі забезпечує конфіденційність корисних даних IP, але не заголовка IP або заголовків розширень, що йдуть перед ESP-заголовком. Крім шифрування корисних даних IP, ESP забезпечує перевірку автентичності і цілісності пакета (заголовок ESP, корисних даних IP і трейлера ESP). Значення перевірки цілісності зберігається в полі «трейлер автентифікації ESP» або «ESP ICV». Заголовок ESP розміщується перед корисними даними IP, а трейлер ESP і трейлер автентифікації ESP поміщаються за корисними даними IP, як показано на рис. 2.20. У разі IPv4 ESP розміщується після IP-заголовка, але перед заголовком протоколу наступного рівня (TCP, UDP, ICMP і т. д.). «Кінцевик ESP» або «Трейлер ESP» містить всі заповнюючі біти, їх довжину і поля наступного заголовка. Якщо для пакета використовується також AH, заголовок ідентифікації застосовується до заголовку ESP, поля Payload, трейлера ESP і ICV.

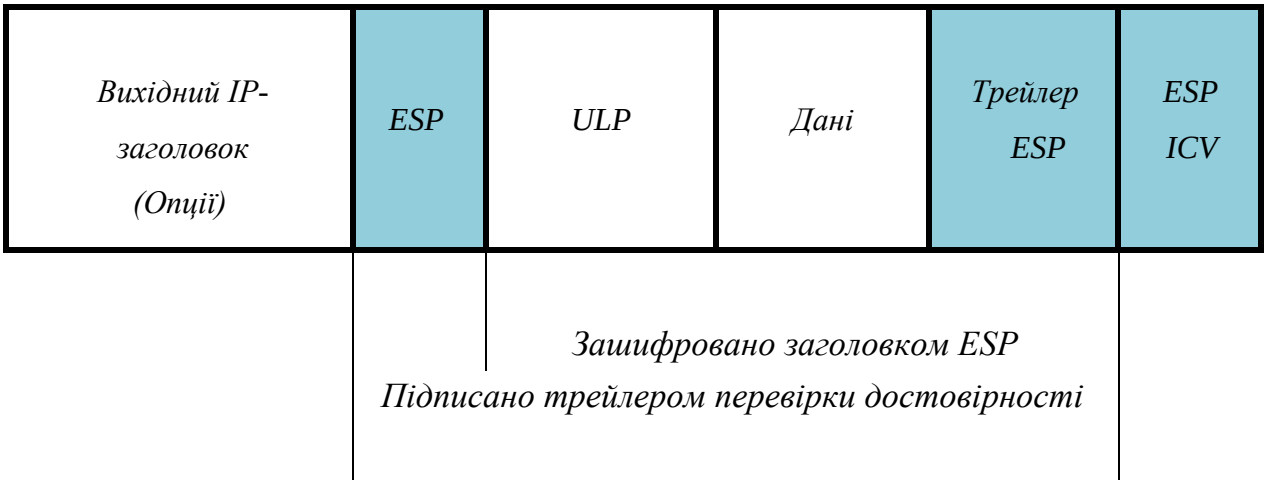

Рис. 2.20 Формат заголовку ESP з IPv4

На рис. 2.21 показаний захист ESP в транспортному режимі в разі IPv6. ESP розглядається як корисне навантаження, що доставляються з кінця в кінець, і повинна з'явитися після даних про пересиланнях, маршрутизації і заголовків розширення фрагментації. Заголовок (заголовки) розширення налаштувань одержувача можуть з'явитися як до, так і після заголовку ESP, залежно від необхідності. Однак у силу того, що ESP захищає тільки поля після заголовка ESP, то в загальному випадку це може бути бажаним — помістити заголовки налаштувань одержувача після заголовку ESP.

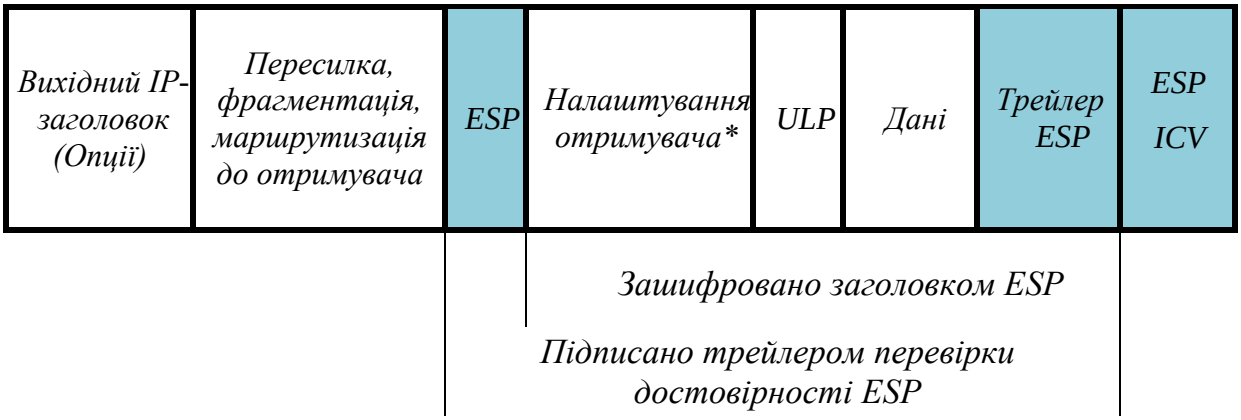

Рис. 2.21 Формат заголовку ESP з IPv6

Захищені дані у випадку тунельного режиму ESP показано на рис. 2.22 і рис. 2.23. У тунельному режимі ESP захищає весь внутрішній IP-пакет, включаючи весь

внутрішній IP-заголовок. ESP в тунельному режимі поміщає вихідний пакет цілком між заголовком ESP і трейлером автентифікації ESP, включаючи заголовок IP, і шифрує дані, створюючи новий заголовок IP.

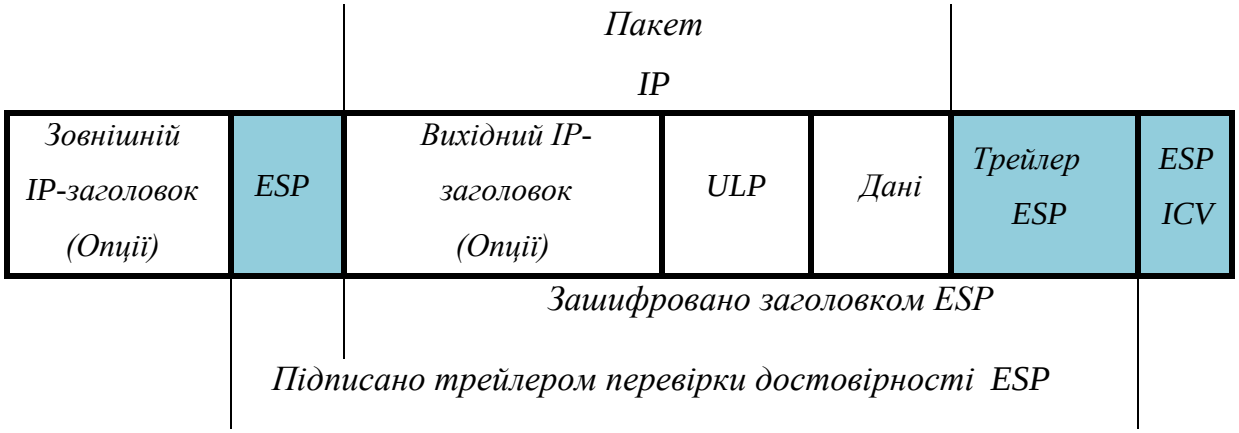

Рис. 2.22 Формат заголовку ESP з IPv4 в тунельному режимі

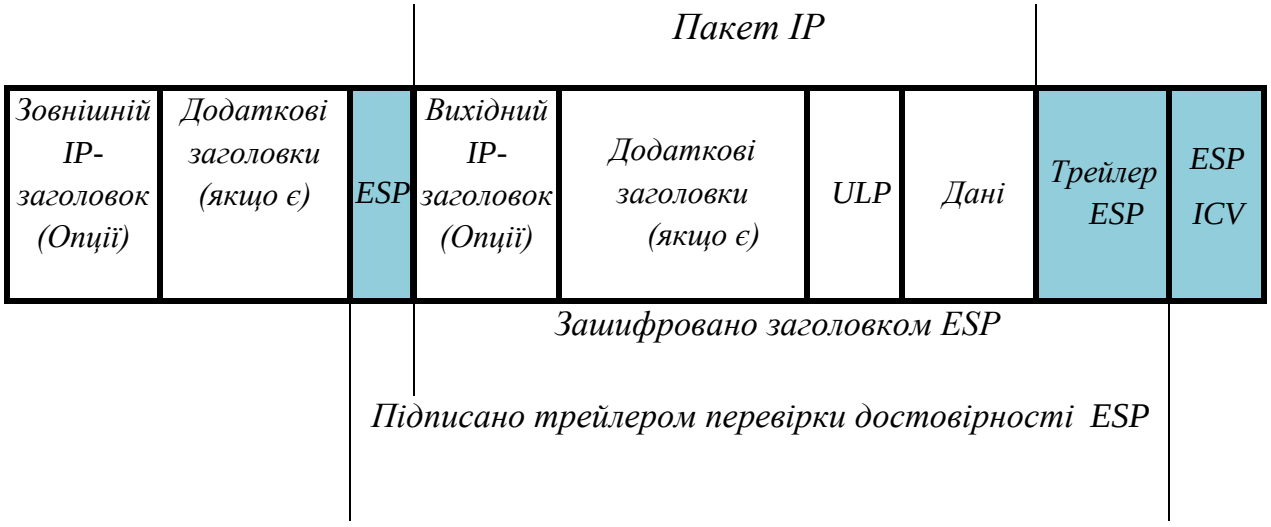

Рис. 2.23 Формат заголовку ESP з IPv6 в тунельному режимі

Таким чином, взаємовідношення між режимами і протоколами IPSec представлені в таблиці 2.1.

Таблиця 2.1.

Взаємовідношення між режимами і протоколами IPSec

Технологія / Режим	Транспортний	Тунельний
AH	Ідентифікує передані дані і окремі частини IP – заголовка	Ідентифікує весь внутрішній IP – заголовок і дані, а також окремі частини IP-заголовка.
ESP	Шифрує і ідентифікує дані, але не IP – заголовок	Шифрує і ідентифікує внутрішній IP – заголовок і дані що передаються

Висновки:

Таким чином, стандарт IPSec, як і інші стандарти та протоколи мережевої безпеки має свої недоліки і є вразливим для атак, але тільки при неправильному його використанні. Та це не є причиною для того, щоб відмовлятися від такого гнучкого і відмінно зарекомендованого інструменту для побудови захищених тунелів.

Деякі рекомендації, яких слід дотримуватися при роботі з IPSec для того, щоб максимально обмежити вплив мережевих атак на збереження, конфіденційність і цілісність інформації наведено нижче:

– Для автентифікації сторін при виборі механізмів автентифікації слід використовувати більш сильний алгоритм SHA і уникати використання менш криптостійких MD5 хешів.

– Для забезпечення конфіденційності переданих даних слід використовувати більш стійкі алгоритми шифрування, наприклад AES.

– Реалізація рішень з допомогою політик IPSec повинна ретельно плануватися, а перед розгортанням – тестуватися в середовищі, що максимально точно моделює реальну.

– IPSec передбачає виключно взаємну автентифікацію партнерів на рівні системи – він не включає перевірку ідентичності користувача цієї системи. Таким чином, якщо зловмисник отримує доступ до системи від імені будь-якого користувача, він може отримати доступ до даних, що передаються за допомогою IPSec. Дана проблема звичайно ж може бути вирішена багатьма стандартними способами ідентифікації користувачів системи – від смарт-карт і біометрії до різних розширень IKE.

РОЗДІЛ 3.
РЕКОМЕНДАЦІЇ НАЛАШТУВАННЯ НАБОРУ ПРОТОКОЛІВ IPSEC НА МЕРЕЖЕВОМУ ОБЛАДНАННІ CISCO

3.1 Підготовка до налаштування та тестування протоколів IPSec на мережевому обладнанні Cisco

Безпечна мережа починається з сильної політики безпеки, яка визначає свободу доступу до інформації та диктує розгортання безпеки в мережі. Cisco Systems пропонує безліч технологічних рішень для створення індивідуального рішення безпеки для Інтернету та мереж віддаленого доступу. Ці масштабовані рішення легко взаємодіють для розгортання мережевої безпеки на підприємстві. IPsec системи Cisco System пропонує ключовий технологічний компонент для забезпечення цілісного рішення безпеки. IPsec від Cisco забезпечує конфіденційність, цілісність та справжність передачі інформації через мережу Інтернет.

Cisco дає змогу користувачам прозоро впроваджувати IPsec в мережеву інфраструктуру, не впливаючи на окремі робочі станції або ПК. Технологія Cisco IPsec доступна у всьому спектрі обчислювальної інфраструктури: Windows 95, Windows NT 4.0 та програмного забезпечення Cisco IOS.

IPsec є основою відкритих стандартів забезпечення безпечного приватного спілкування через Інтернет. На основі стандартів, розроблених Internet Engineering Task Force (IETF), IPsec забезпечує конфіденційність, цілісність та достовірність передачі даних через загальнодоступну мережу. IPsec забезпечує необхідний компонент стандартного, гнучкого рішення для розгортання політики безпеки в масштабах всієї мережі.

Cisco IPsec включає наступні технології:

- IPsec - використовує технологію шифрування для забезпечення конфіденційності даних, цілісності та достовірності між одноранговими учасниками

приватної мережі. Cisco забезпечує повну підтримку корисного навантаження для інкапсуляції безпеки (ESP) та заголовка аутентифікації (AH).

- Інтернет-обмін ключами (IKE) - забезпечує управління асоціацією безпеки. IKE засвідчує аутентифікацію кожного однорангового в транзакції IPsec, узгоджує політику безпеки та обмінюється обміном ключами сеансу. Компанія Cisco доклала зусиль щодо стандартизації IKE, написавши чернетки IETF в Інтернеті та зробивши безкоштовну версію IKE доступною в Інтернеті. Докладніше див. У розділі "Протокол захисту обміну ключами в Інтернеті (IKE)".
- Управління сертифікатами. Cisco підтримує сертифікати X509.V3 для аутентифікації пристроїв під час узгодження IKE. Управління сертифікатами включає використання простого протоколу реєстрації сертифікатів (SCEP), протоколу для спілкування з органами з сертифікації (CA). Це рішення сертифікатів підтримує ієрархічну структуру сертифікатів та перехресну сертифікацію, необхідну для рішення інфраструктури відкритих ключів (PKI).

До компонентних технологій належать наступні:

– Діффі-Хеллман - це криптографічний протокол з відкритим ключем, який дозволяє двом сторонам встановити спільну таємницю через незахищений канал зв'язку. IKE використовує Diffie-Hellman для встановлення ключів сесії. Центр рішень VPN підтримує дві групи Diffie-Hellman: Group 1 - група MODP з 768-бітовим модулем; Group 2 - група MODP з 1024-бітовим модулем.
– DES - стандарт шифрування даних, який використовується для шифрування пакетних даних.
– Алгоритми MD5 / SHA - ідентифікують пакетні дані.

3.2 Налаштування параметрів IPSec

Етапи налаштування і встановлення з'єднання IPSec:

– Перша фаза – встановлення захищеного з'єднання через небезпечну мережу для подальшої процедури обміну:

- Створення політики безпеки ISAKMP.

– Друга фаза – узгодження всіх параметрів, асоційованих з загальним каналом SA:

- Створення політики безпеки IPSec.
- Створення списку доступу (ACL).
- Створення крипто-карти (Crypto map).

– Запуск і перевірка роботи IPSec з'єднання.

Загальний набір параметрів безпеки IPSec називається політикою IPSec. Політика складається з набору правил, що визначають обробку мережевого трафіку. Кожне правило містить набір фільтрів та дії, які це правило буде виконувати з пакетом, відповідно умовам фільтру. В якості параметрів фільтрів можуть бути задані IP-адреси, адреси мережі або повне доменне ім'я відправника і одержувача пакета, тип IP-протоколу (ICMP, TCP, UDP, тощо), номери TCP і UDP портів відправника і одержувача.

У Cisco IOS налаштування IPSec відбувається в CLI наступним чином:

В режимі глобальної конфігурації:

R0 (config) #crypto isakmp policy [номер] – створюємо політику підключення 1-ї фази,

R0 (config-isakmp) #authentication [параметри] – задаємо метод автентифікації:

– pre-share – метод загального ключа,
– rsa-encr – метод Rivest-Shamir-Adleman Encryption,
– rsa-sig – метод Rivest-Shamir-Adleman Signature.

R0 (config-isakmp) #hash – задаємо алгоритм хешування:

– md5 – алгоритм Message Digest 5,
– sha – алгоритм Secure Hash Standard,
– sha256 – алгоритм Secure Hash Standard 2 (256 bit),
– sha384 – алгоритм Secure Hash Standard 2 (384 bit),
– sha512 – алгоритм Secure Hash Standard 2 (512 bit).

R0 (config-isakmp) #encryption – задаємо метод шифрування (та довжину ключа):

- 3des – алгоритм Three key triple DES (ключ 3x56 біт),
- aes – алгоритм AES – Advanced Encryption Standard (ключ 128, 192, 256 біт),
- des – алгоритм DES – Data Encryption Standard (ключ 56 біт).

R0 (config-isakmp) #group – задаємо групу Diffie-Hellman, яка буде використовуватися для безпечного обміну ключами:

- Diffie-Hellman group 1 (768 bit)
  - 14 Diffie-Hellman group 14 (2048 bit)
  - 15 Diffie-Hellman group 15 (3072 bit)
  - 16 Diffie-Hellman group 16 (4096 bit)
  - 19 Diffie-Hellman group 19 (256 bit ecp)
- Diffie-Hellman group 2 (1024 bit)
  - 20 Diffie-Hellman group 20 (384 bit ecp)
  - 21 Diffie-Hellman group 21 (521 bit ecp)
  - 24 Diffie-Hellman group 24 (2048 bit, 256 bit subgroup)
- Diffie-Hellman group 5 (1536 bit).

R0 (config-isakmp) #lifetime [секунди] – задаємо час життя підключення,

R0 (config) #crypto isakmp key [ключ] address [IP-адреса] – задаємо ключ підключення і вказуємо IP-адресу віддаленого маршрутизатора.

Приклад CLI налаштування на обладнанні Cisco, рис.3.1.

```
R0(config)#
R0(config)#crypto isakmp policy 1
R0(config-isakmp)#authentication pre-share
R0(config-isakmp)#hash sha
R0(config-isakmp)#encryption aes 256
R0(config-isakmp)#group 5
R0(config-isakmp)#lifetime 180
R0(config-isakmp)#exit
R0(config)#crypto isakmp key PASS address 192.168.0.1
R0(config)#
```

Рис. 3.1 Налаштування 1-ї фази

Конфігуруємо 2 фазу IPSec:

R0 (config) #crypto IPSec transform-set [назва] {параметри} – створюємо transform-set для маршрутизатора R0:

Режим роботи тільки з автентифікаційним заголовком AH:

- ah-md5-hmac – режим AH-HMAC-MD5,
- ah-sha-hmac – режим AH-HMAC-SHA,
- ah-sha256-hmac – режим AH-HMAC-SHA256,
- ah-sha384-hmac – режим AH-HMAC-SHA384,
- ah-sha512-hmac – режим AH-HMAC-SHA512.

Режим роботи тільки з зашифрованими даними ESP:

- esp-3des – режим ESP transform using 3DES(EDE) cipher (168 bits),
- esp-aes – режим ESP transform using AES cipher,
- esp-des – режим ESP transform using DES cipher (56 bits),
- esp-seal – режим ESP transform using SEAL cipher (160 bits).

Режим роботи автентифікаційного заголовка AH для ESP режиму:

- esp-md5-hmac – режим ESP transform using HMAC-MD5 auth,
- esp-sha-hmac – режим ESP transform using HMAC-SHA auth,
- esp-sha256-hmac – режим ESP transform using HMAC-SHA256 auth,
- esp-sha384-hmac – режим ESP transform using HMAC-SHA384 auth,
- esp-sha512-hmac – режим ESP transform using HMAC-SHA512 auth.

R0 (config) #access-list [номер] permit ip {параметри} – створюємо список доступу, який буде визначати в яких ситуаціях пакети будуть потрапляти в IPSec тунель,

R0 (config) #crypto map [назва] {номер} IPSec-isakmp – створюємо так звану крипто карту з номером. Номер використовується для того, щоб можна було створювати кілька підключень, тобто можна їх створювати одна за одною для всіх наших тунелів. Не треба плутати з політиками, там номер каже про пріоритет підключення, тут це просто номер і не несе якогось смислового навантаження,

R0 (config-crypto-map) #set peer [ip-адреса] – вказуємо ip адресу віддаленого маршрутизатора,

R0 (config-crypto-map) #match address [номер ACL] – застосовуємо створений раніше список доступу,

R0 (config-crypto-map) #set transform-set [назва] – застосовуємо створений раніше transform-set.

Приклад CLI налаштування 2-ї фази на обладнанні Cisco, рис. 3.2.

```
R0(config)#
R0(config)#crypto ipsec transform-set IPSec ah-sha-hmac esp-aes esp-sha-hmac
R0(config)#access-list 100 permit ip 192.168.0.0 0.0.0.3 192.168.1.0 0.0.0.3
R0(config)#
R0(config)#crypto map IPSec-map 2018 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
R0(config-crypto-map)#set peer 192.168.0.2
R0(config-crypto-map)#match address 100
R0(config-crypto-map)#set transform-set IPSec
R0(config-crypto-map)#exit
R0(config)#
R0(config)#interface fastEthernet 0/0
R0(config-if)#crypto map IPSec-map
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R0(config-if)#
```

Рис. 3.2 Налаштування 2-ї фази

Застосовуємо створену крипто карту для інтерфейсів:

R0 (config) #interface [назва] – заходимо в налаштування порту, що виходить у зовнішню мережу,

R0 (config-if) #crypto map [назва] – застосовуємо до нього крипто карту.

3.3 Тестування швидкодії протоколу IPSec в емуляційному програмному середовищі та на реальному обладнанні

Тестування проводилося в емуляційному програмному середовищі та на реальному обладнанні, маршрутизатори Cisco 2800. Віртуальна лабораторія EVE-NG, з наступним програмним забезпеченням Cisco: c7200-adventerprisek9-mz.152-4.S6.bin

У віртуальному середовищі EVE-NG було створену мережу з чотирьох маршрутизаторів Cisco 7200 та двох комп’ютерів, рис. 3.3. Файл, обсяг якого становив 52 Мбайт, передавався по мережі з різними налаштуваннями IPSec в транспортному режимі (Transport Mode) між двома комп'ютерами з операційною системою Linux, а також без використання захисту IPSec.

В транспортному режимі, шифрування та хешування відбувається лише з корисними даними, а не з усім пакетом, як це відбувається в тунельному режимі.

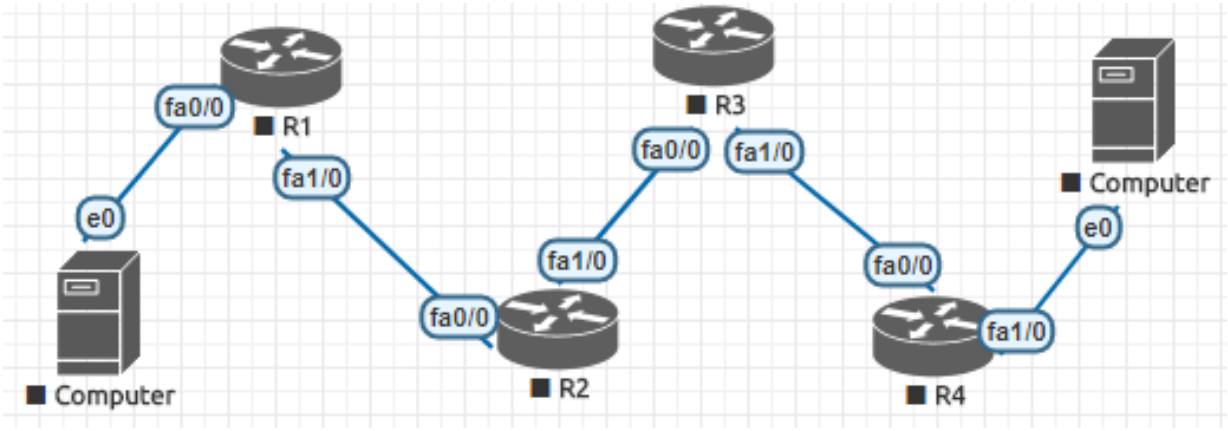

Рис. 3.3 Схема підключення обладнання в EVE-NG

На реальному обладнанні було створено мережу з двох маршрутизаторів Cisco 2800 та двох комп’ютерів, рис. 3.4. Файл, обсяг якого становив 245 Мбайт, передавався по мережі з різними налаштуваннями IPSec, а також без використання захисту IPSec, в транспортному режимі (Transport Mode) між двома комп'ютерами з операційною системою Windows 10.

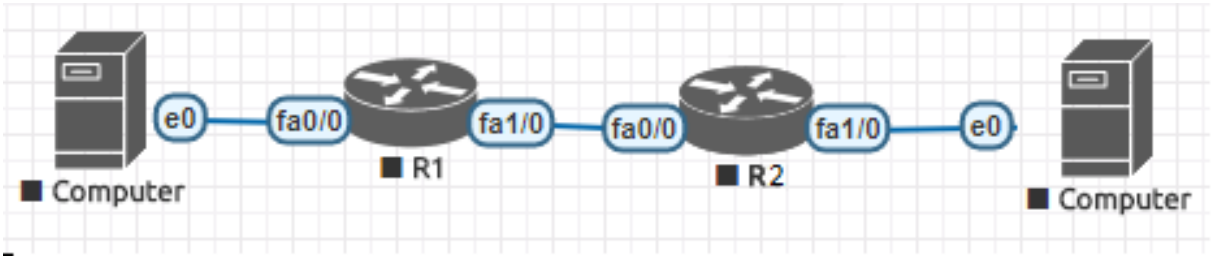

Рис. 3.4 Схема підключення реального обладнання Cisco

Результати досліду у віртуальному середовищі

У вимірах можлива деяка похибка, так як вимірювання завантаженості процесора і часу передачі файлу проводилися з допомогою утиліти моніторингу стану Linux – htop.

1. Передача файлу по мережі без використання IPSec. Час передачі файлу в середньому склав 9 с, а середня швидкість передачі даних досягла 52,85 Мбіт/с. При цьому завантаженість процесорів на склала 8.1%, як показано на рис. 3.5.

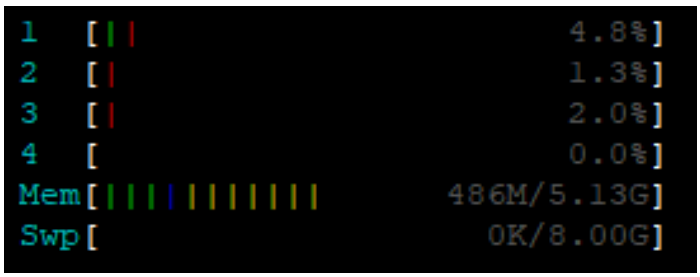

Рис. 3.5 Навантаження процесорів без використання IPSec

2. Передача файлу по мережі з налаштованою політикою IPSec, з використанням фільтра для забезпечення цілісності даних (протокол AH з використанням SHA-1). При цьому час передачі даних зріс незначно, до 10 с, а швидкість незначно змінилася, до 47,34 Мбіт/с. При цьому також дещо зросло завантаження процесорів до 12.9%, як показано на рис. 3.6.

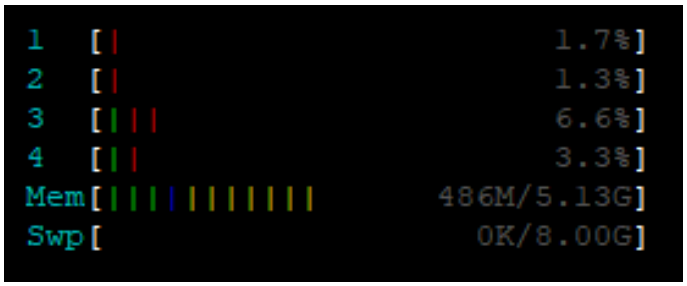

Рис. 3.6 Навантаження процесорів при AH SHA1

3. Передача файлу по мережі з налаштованою політикою IPSec, із застосуванням фільтра ESP без використання AH, з шифруванням за допомогою алгоритму DES і хешуванням MD5. Значних змін у продуктивності в цій конфігурації порівняно з попередніми не сталося. Час передачі файлу зріс до 11 с, а

швидкість передачі склала 43,56 Мбіт/с. Навантаження процесорів склало 17.6% відповідно, і показана на рис. 3.7.

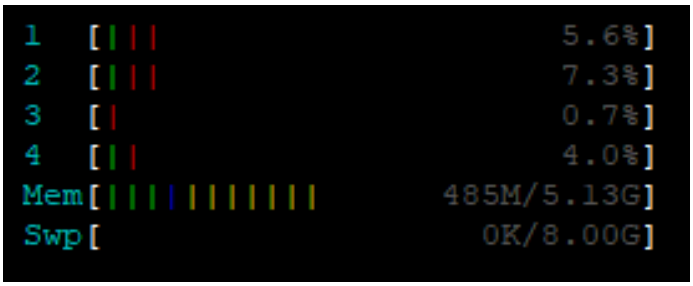

Рис. 3.7 Навантаження процесорів при AH MD5 та ESP DES

DES є застарілим алгоритмом і не рекомендується до використання там, де захищаються дані мають велику цінність, але стійкість цього алгоритму може бути значно покращено завдяки більш частій зміні ключа.

4. Передача файлу по мережі з налаштованою політикою безпеки IPSec, із застосуванням фільтра ESP, використовує шифрування за допомогою алгоритму 3DES, замість алгоритму DES, і хешування MD5. При цьому час передачі файлу зріс і склав 12 с, а швидкість передачі файлу відповідно 39,62 Мбіт/с. Рівень завантаження процесорів при цьому склав 22.7% і показаний на рис. 3.8.

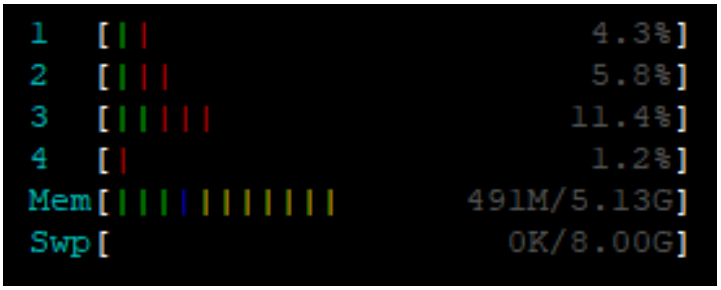

Рис. 3.8 Навантаження процесорів при AH MD5 та ESP 3DES

5. Передача файлу по мережі з налаштованою політикою безпеки IPSec, із застосуванням фільтра ESP з 3DES і SHA1. При цьому час передачі файлу склав 13 с, а швидкість передачі файлу 35,09 Мбіт/с відповідно. Рівень завантаження процесорів при цьому склав 27.3%, як показано на рис. 3.9.

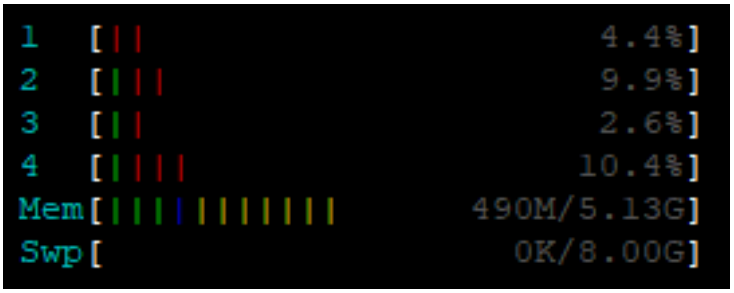

Рис. 3.9 Навантаження процесорів при AH SHA1 та ESP 3DES

6. Передача файлу по мережі з налаштованої політикою безпеки IPSec, з використанням протоколу ESP AES 256 спільно з протоколом AH SHA512. При цьому найбільш безпечною, а отже, найбільш ресурсоємною конфігурацією, доступною в даній Cisco IOS, отримані наступні результати: час передачі збільшився до 22 с, швидкість впала до 23,92 Мбіт/с. Завантаження процесорів склало 116.7% відповідно, і показано на рис. 3.10.

Рис. 3.10 Навантаження процесорів при AH SHA512 та ESP AES256

Порівняння часу передачі даних, залежно від алгоритмів, що застосовуються, рис. 3.11:

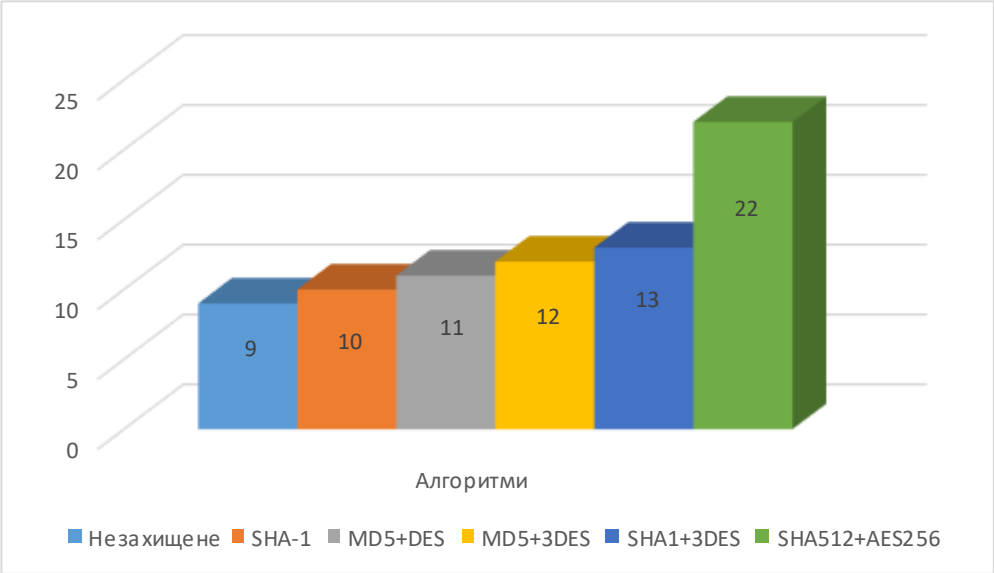

Рис. 3.11 Час передачі даних IPSec

Порівняння швидкості передачі даних, залежно від алгоритмів, що застосовуються, представлено на рис. 3.12.

А порівняння навантаження процесорів мережевого обладнання Cisco, залежно від алгоритмів, що застосовуються, представлено на рис. 3.13.

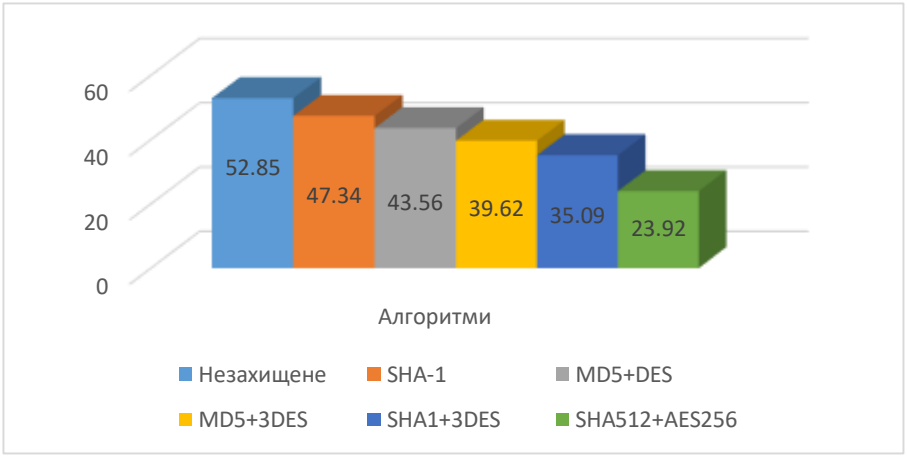

Рис. 3.12 Швидкість передачі даних IPSec

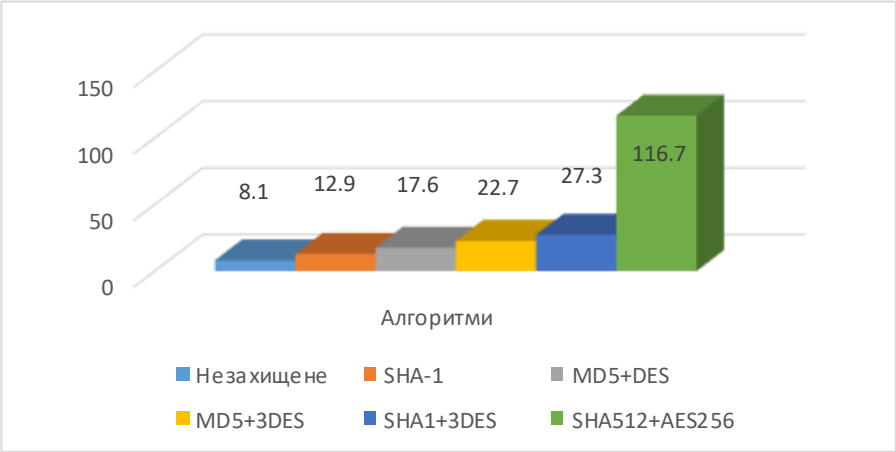

Рис. 3.13 Навантаження процесора IPSec

Результати досліду на реальному обладнанні Cisco

У вимірах можлива деяка похибка, так як вимірювання завантаженості процесора і часу передачі файлу проводилися з допомогою утиліти моніторингу стану Cisco та диспетчера завдань Windows 10.

1. Передача файлу по мережі без використання IPSec. Час передачі файлу склав 25 с, а середня швидкість передачі даних становить 98,85 Мбіт/с, при цьому завантаженість процесорів склала 20%, як показано на рис. 3.14.

2. Передача файлу по мережі з налаштованою політикою IPSec, з використанням фільтру для забезпечення цілісності даних (протокол AH з використанням SHA-1). При цьому час передачі даних зріс до 51 с, а швидкість зменшилася до 40,2 Мбіт/с, при цьому також зросло навантаження процесора до 80%, як показано на рис. 3.15.

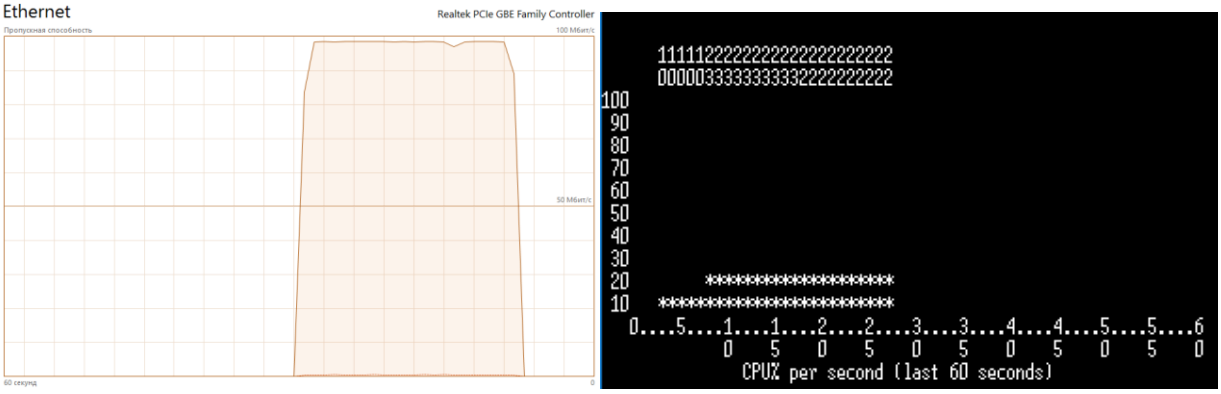

Рис. 3.14 Швидкість передачі та навантаження процесора без використання IPSec

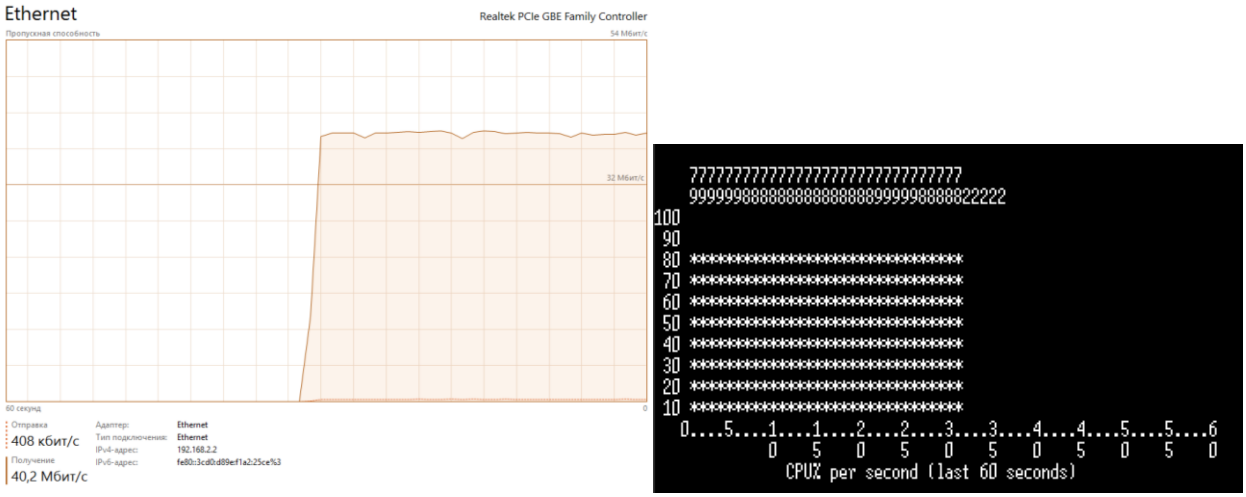

Рис. 3.15 Швидкість передачі та навантаження процесора при AH SHA1

3. Передача файлу по мережі з налаштованою політикою IPSec, із застосуванням фільтра ESP без використання AH, з шифруванням за допомогою алгоритму DES і хешуванням MD5. Значних змін у продуктивності в цій конфігурації порівняно з попередніми не сталося. Час передачі файлу зріс до 70 с, а швидкість передачі склала 30,6 Мбіт/с. Навантаження процесорів в межах 80% відповідно, і показана на рис. 3.16.

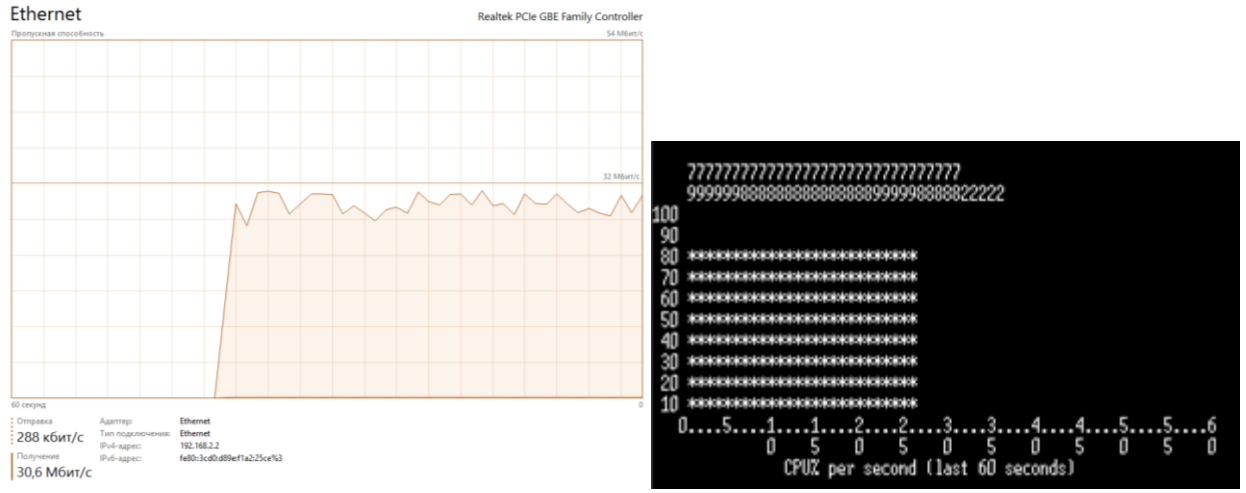

Рис. 3.16 Швидкість передачі та навантаження процесора при ESP MD5 DES

DES є застарілим алгоритмом і не рекомендується до використання там, де захищаються дані мають велику цінність, але стійкість цього алгоритму може бути значно покращено завдяки більш частій зміні ключа.

4. Передача файлу по мережі з налаштованою політикою безпеки IPSec, із застосуванням фільтра ESP, використовує шифрування за допомогою алгоритму 3DES, замість алгоритму DES, і хешування SHA1. При цьому час передачі файлу зменшився і склав 64 с, а швидкість передачі файлу відповідно 32,9 Мбіт/с. Рівень завантаження процесорів при цьому залишився в межах 80% і показаний на рис. 3.17.

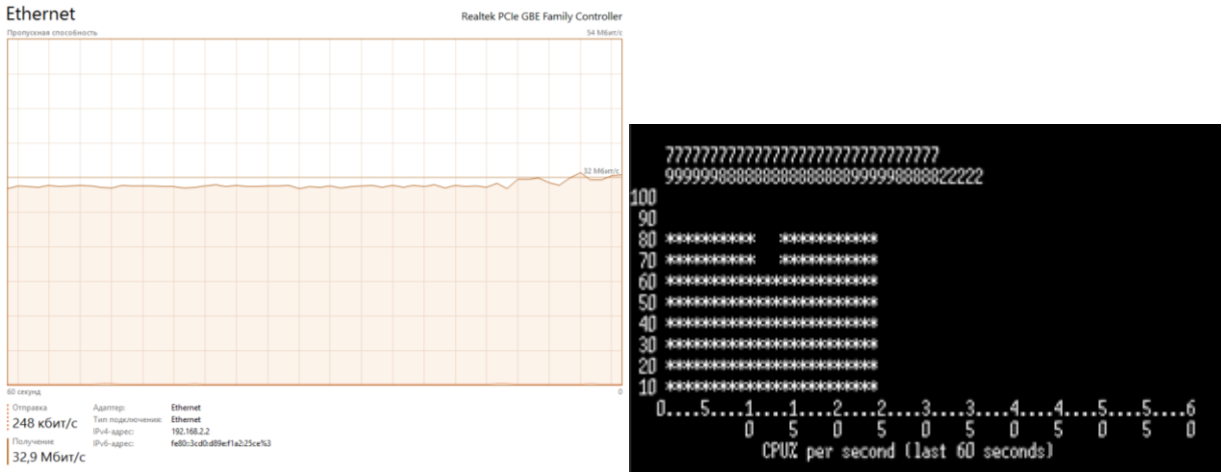

Рис. 3.17 Швидкість передачі та навантаження процесорів при AH SHA1 та ESP 3DES

5. Передача файлу по мережі з налаштованою політикою безпеки IPSec, із застосуванням фільтра AH SHA1 та ESP з AES 128 біт ключем і SHA1. При цьому час передачі файлу склав 84 с, а швидкість передачі файлу 24,5 Мбіт/с відповідно. Рівень завантаження процесорів при цьому залишився в межах 80%, як показано на рис. 3.18.

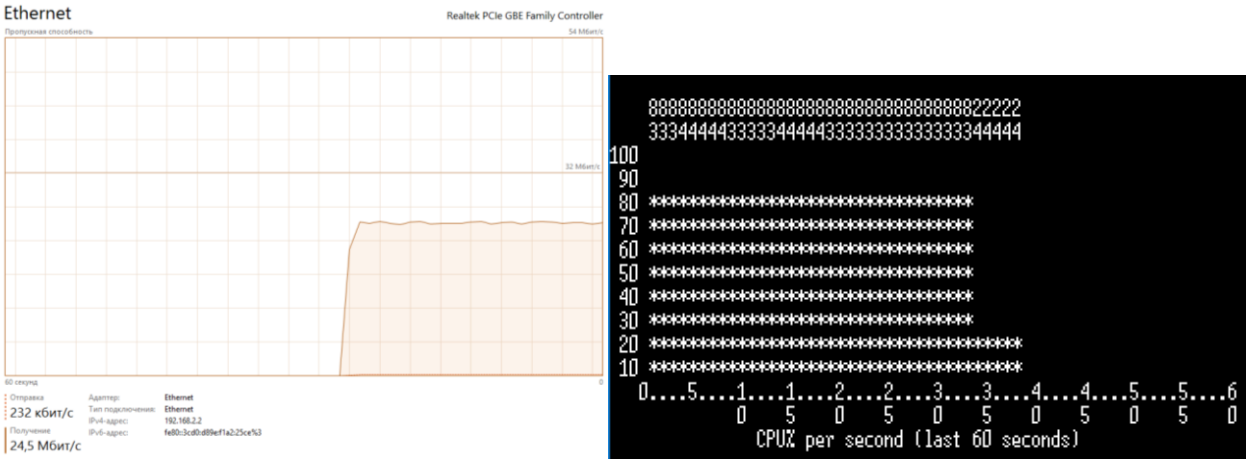

Рис. 3.18 Швидкість передачі та навантаження процесорів при AH SHA1 та ESP SHA1 AES128

6. Передача файлу по мережі з налаштованої політикою безпеки IPSec, з використанням протоколу ESP SHA1 і AES 256 спільно з протоколом AH SHA1. При цьому найбільш безпечною, а отже, найбільш ресурсоємною конфігурацією, доступною в даній Cisco IOS, отримані наступні результати: час передачі збільшився до 88 с, швидкість впала до 23,2 Мбіт/с. Завантаження процесорів залишилось в межах 80% відповідно, і показано на рис. 3.19.

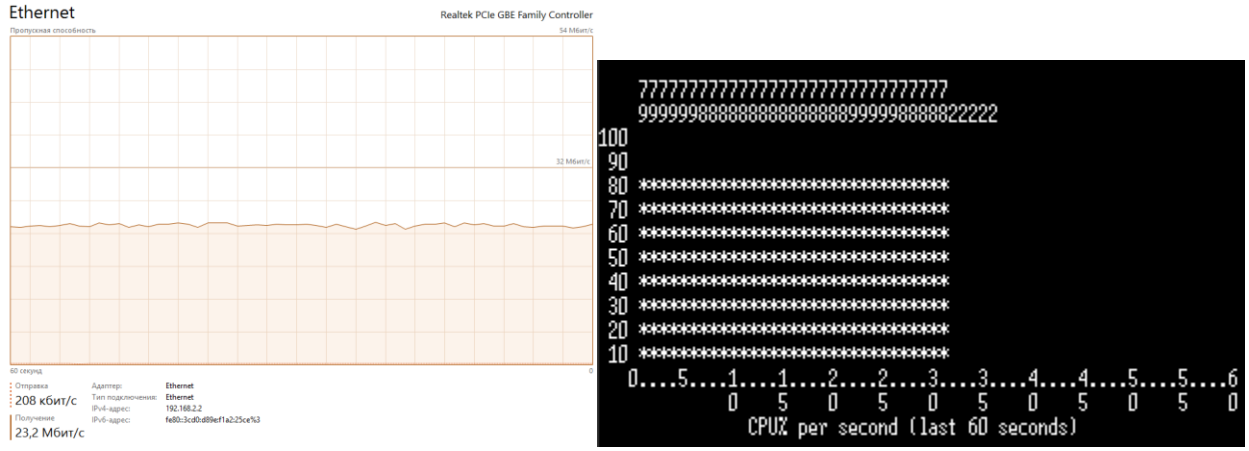

Рис. 3.19 Швидкість передачі та навантаження процесорів при AH SHA1 та ESP SHA1 AES256

Порівняння часу передачі даних, залежно від алгоритмів, що застосовуються, рис. 3.20:

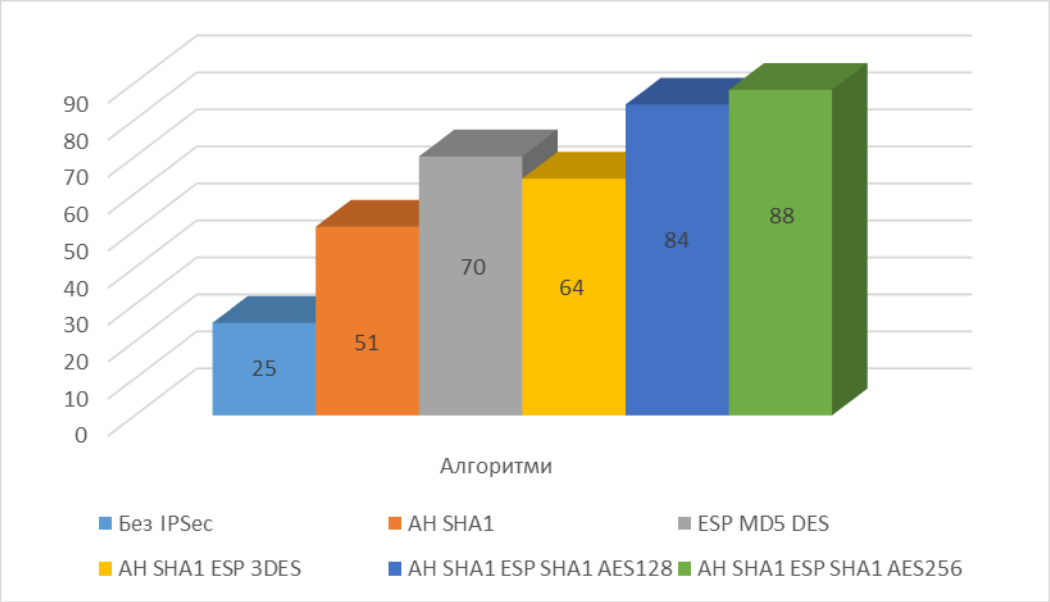

Рис. 3.20 Час передачі даних IPSec

Порівняння швидкості передачі даних, залежно від алгоритмів, що застосовуються, рис. 3.21:

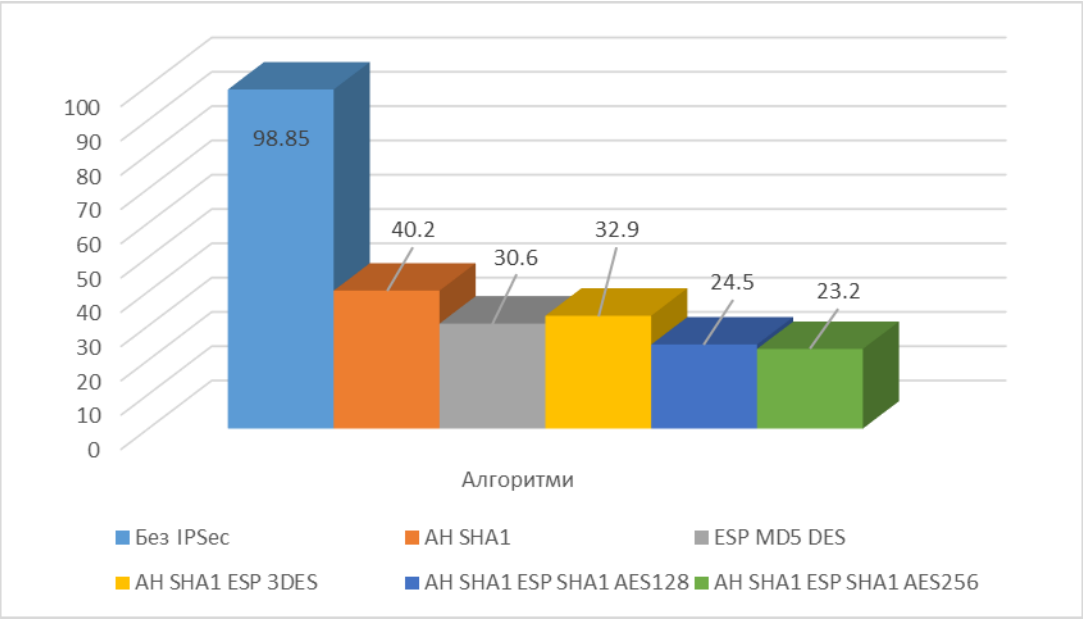

Рис. 3.21 Швидкість передачі даних IPSec

Порівняння навантаження процесорів мережевого обладнання Cisco, залежно від алгоритмів, що застосовуються, рис. 3.22:

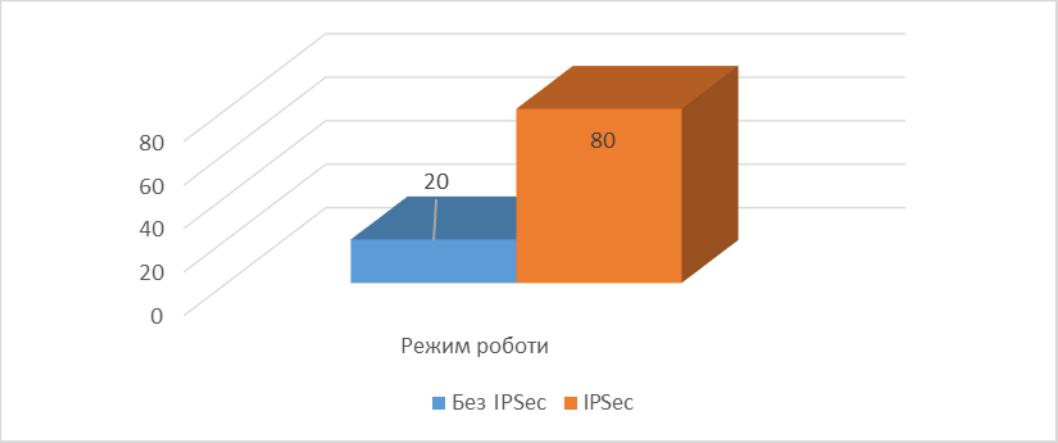

Рис. 3.22 Навантаження процесора IPSec

Результати тестування показують, що ресурсоємність IPSec невисока тільки при використанні протоколу AH MD5 і при використанні протоколу ESP з алгоритмом шифрування DES. При використанні протоколу ESP з більш сильним алгоритмом шифрування 3DES чи AES, продуктивність значно знижується, але можливість застосовувати застарілі процесори не виключається, при цьому жертвуючи швидкістю передачі даних. На реальному обладнанні змін зазнали лише швидкість передачі даних, навантаження на процесор майже завжди залишалось однаковим при застосування різних алгоритмів. Таким чином, IPSec може бути рекомендований для використання у багатьох мережах в цілях підвищення безпеки.

Висновки:

В ході роботи було проведено налаштування та тестування продуктивності протоколу IPSec на обладнанні Cisco, для того, щоб виявити рівень навантаження на центральний процесор під час передачі даних по мережі з використанням різних криптографічних алгоритмів.

За результатами тестування бачимо, що загалом технологія IPSec досить ресурсоємна, за винятком використання деяких застарілих криптографічних алгоритмів, таких як засіб автентифікації MD5 та алгоритм шифрування DES. При використанні протоколу ESP з більш сильним алгоритмом шифрування AES та ключем 128, 192 та 256 біт, продуктивність значно знижується, але, тим не менш, при низьких швидкостях передачі даних продуктивності навіть застарілих процесорів буде достатньо. У випадках, де потрібна висока швидкість обміну даними, може виявитися достатнім використання алгоритму DES із частою зміною ключа.

Таким чином, IPSec може бути рекомендований для використання у багатьох мережах в цілях підвищення безпеки.

ЗАГАЛЬНІ ВИСНОВКИ ПО РОБОТІ

В дипломній роботі проведено аналіз основних загроз інформаційної безпеки, визначено основні і найбільш поширені в даний час системи та протоколи безпеки, що забезпечують захист персональних даних користувачів від несанкціонованого доступу, вірусних атак та неправомірного використання.

Програмно-технічні засоби забезпечення інформаційної безпеки є основою системи захисту інформації. Це сукупність алгоритмів, програм і протоколів, що забезпечують шифрування, контроль за НСД, захист від шкідливих програм і багато іншого.

Проаналізовано переваги та недоліки найбільш використовуваних протоколів захисту передачі даних IPSec та SSL. Проведено порівняльний аналіз даних протоколів та узагальнення результатів у вигляді порівняльної таблиці.

Основну увагу приділено протоколам IPSec, так як вони найчастіше використовується у більшості реалізацій віртуальних приватних мереж. На сьогоднішній час на ринку представлені як програмні реалізації (наприклад, протокол реалізований в операційній системі IOS компанії Cisco), так і програмно-апаратні реалізації. Проведено аналіз структури даних протоколів.

Розкрито принципи роботи протоколів IPSec при передачі даних по мережі з використанням механізмів захисту, реалізованих цими протоколами.

Розглянуто режими роботи асоціацій безпеки, випадки, для яких необхідне застосування того чи іншого режиму, а також захист даних з допомогою IPSec для IPv4 і IPv6.

Описано принцип та особливості роботи AH і ESP у транспортному та тунельному режимі, а також, наведена порівняльна таблиця роботи даних протоколів при різних режимах.

В дипломній роботі надано рекомендації по найбільш ефективному використанню цих протоколів з максимальним обмеженням впливу мережевих атак на збереження, конфіденційність і цілісність інформації.

В третьому розділі роботи проведено налаштування та тестування продуктивності протоколу IPSec на мережевому обладнанні Cisco, для того, щоб виявити рівень навантаження на центральний процесор під час передачі даних по мережі з використанням різних криптографічних алгоритмів. Робота виконана на двох програмних середовищах: емуляційному та реальному обладнанні. Проведено порівняння по часу, швидкості передачі даних та навантаженню процесора та представлено результати роботи мережевого обладнання Cisco і швидкості передачі даних при використанні протоколів безпеки IPSec з різними комбінаціями алгоритмів шифрування, способів автентифікації і механізмів забезпечення цілісності даних.

Проведений аналіз показав, що для використання більш потужних і стійких алгоритмів захисту інформації потрібні більш продуктивні процесори. В іншому випадку час передачі даних буде збільшуватися, що може негативно позначитися на продуктивності роботи мережі.

За результатами тестування можна відзначити, що технологія IPSec ресурсоємна, за винятком використання деяких застарілих криптографічних алгоритмів, таких як засіб автентифікації MD5 та алгоритм шифрування DES. При використанні протоколу ESP з більш сильним алгоритмом шифрування AES та ключем 128, 192 та 256 біт, продуктивність значно знижується, але, тим не менш, при низьких швидкостях передачі даних продуктивності навіть застарілих процесорів буде достатньо. У випадках, де потрібна висока швидкість обміну даними, може виявитися достатнім використання алгоритму DES із частою зміною ключа.

Таким чином, IPSec може бути рекомендований, для використання у різних мережа, в цілях підвищення безпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Інформаційно-аналітичне забезпечення фінансово-економічної безпеки діяльності підприємства / [Електронний ресурс]. https://www.bibliofond.ru/view.aspx?id=824421 (дата звернення: 01.05.2020)

2. Аналіз кредитних операцій комерційного банку/ [Електронний ресурс]. URL: https://ukrbukva.net/page,17,92042-Analiz-kreditnyh-operaciiy-kommercheskogo-banka-na-primere-OOO-MFO-Kaspiiyskiiy-kapital.html (дата звернення: 01.05.2020)

3. Правове і нормативне забезпечення захисту інформації/ [Електронний ресурс]. URL: http://bukvar.su/gosudarstvo-i-pravo/page,2,183384-Pravovoe-i-normativnoe-obespechenie-zashity-informacii.html (дата звернення: 08.05.2020)

4. Правове і нормативне забезпечення захисту інформації// електрон. текст. дані URL: http://ukrefs.com.ua/page,3,183384-Pravovoe-i-normativnoe-obespechenie-zashity-informacii.html (дата звернення: 08.05.2020)

5. Забезпечення захисту інформації / [Електронний ресурс]. URL: http://bukvar.su/gosudarstvo-i-pravo/183384-Pravovoe-i-normativnoe-obespechenie-zashity-informacii.html (дата звернення: 01.05.2020)

6. Інформаційна безпека розподілених систем. Рекомендації X.800. Частина 2. / Мережеві механізми безпеки // [Електронний ресурс]. URL: http://ni.biz.ua/3/3_6/3_64709_informatsionnaya-bezopasnost-raspredelennih-sistem-rekomendatsii-X-chast--setevie-mehanizmi-bezopasnosti.html (дата звернення: 08.05.2020)

7. Інформаційна безпека / [Електронний ресурс]. URL: http://uadoc.zavantag.com/text/19202/index-12.html (дата звернення: 08.05.2020)

8. Безпека комп’ютерних мереж / [Електронний ресурс]. URL: https://svitppt.com.ua/informatika/bezpeka-kompyuternih-merezh.html (дата звернення: 08.05.2020)

9. Стандартизація технології безпеки інформаційних систем / [Електронний ресурс]. URL: https://ukrbukva.net/page,3,98752-Standartizaciya-tehnologii-bezopasnosti-informacionnyh-sistem.html (дата звернення: 08.05.2020).

10. IPSECURITY / [Електронний ресурс]. URL: https://bigedu.ru/referats/nformatika/4238-ipsecurity.html (дата звернення: 03.05.2020)

11. Левченко О.М. / Інформаційна безпека держави, суспільства та особистості, 2015. – 155 с. (дата звернення: 01.05.2020).

12. Система захисту інформації в локальній мережі підприємства / [Електронний ресурс]. URL: https://ukrbukva.net/page,8,97241-Sistema-zashity-informacii-v-lokal-noiy-seti-predpriyatiya.html (дата звернення: 03.05.2020).

13. Забезпечення цілісності та автентичності даних в IP-мережах з використанням протоколу AH (IPSec) / [Електронний ресурс]. URL: https://studfile.net/preview/5993348/page:40/ (дата звернення: 09.05.2020).

14. IPSec / [Електронний ресурс]. https://uk.m.wikipedia.org/wiki/IPsec (дата звернення: 09.05.2020).

15. Вступ до вивчення політик IPSec / [Електронний ресурс]. URL: https://jak.waykun.com/articles/vstup-do-vivchennja-politik-ipsec.htmll (дата звернення: 15.05.2020).

16. Налаштування клієнта для з'єднання за протоколом IPSec між ОС Linux на основі сервера доступу racoon і ОС Windows XP/Windows – 2000 з використанням сертифікатів X.509 і протоколу обміну ключами ISAKMP на стороні ОС Windows XP/Windows – 2000 / [Електронний ресурс]. дані URL: https://mylektsii.ru/11-22171.html (дата звернення: 15.05.2020).

17. Побудова локальної обчислювальної мережі на основі VPN технологій / [Електронний ресурс]. URL: https://ukrbukva.net/page,17,94071-Postroenie-lokal-noiy-vychislitel-noiy-seti-na-osnove-VPN-tehnologiiy.html (дата звернення: 12.05.2020) .

18. Захарченко М.В. Інформаційна безпека інформаційно-комунікаційних систем. Захист інформації від НСД у каналах зв’язку: навч. посіб. / М.В. Захарченко, В.В. Топалов, М.С. Русляченко // За ред. чл.-кор. МАЗ В.Г. Кононовича. – Одеса: ОНАЗ ім. О.С. Попова, 2011. – 228 с. (дата звернення: 5.05.2020)

19. IPSec / [Електронний ресурс]. URL: https://studfile.net/preview/5157571/page:4/ (дата звернення: 11.05.2020)

20. Реалізація протоколу IPSec у різних операційних системах для побудови захищених віртуальних мереж / [Електронний ресурс]. URL: http://dspace.nbuv.gov.ua/bitstream/handle/123456789/26535/01-Kornienko.PDF?sequence=1 (дата звернення: 10.05.2020)

21. Canasan J. Fundamentals of IPSec / John E. Canavan. – Boston • London: Artech House, 2001. – 218 с. 5-18 (дата звернення 14.05.2020)

22. W. Obom. Official Exam Certification Guide, 2nd Edirion. Cisco Press, 2007. – 207 с. 1-14 (дата звернення 01.05.2020)

23. У. Блэк / Интернет: протоколы безопасности, 2001. (дата звернення 11.05.2020)

24. Крейг Хант / TCP/IP / Сетевое администрирование, 2008. (дата звернення 13.05.2020)

25. Стопинге Вильям / Современные компьютерные сети, 2003. (дата звернення 06.05.2020)

26. Фейт Сидни / TCP/IP / Архитектура, протоколы, реализация, 2000. (дата звернення 11.05.2020).

27. Найк Дилип / Стандарты и протоколы Интернета, 1999. (дата звернення 09.05.2020)

28. Блэк Уилесс / Интернет: протоколы безопасности, 2001. (дата звернення 11.05.2020)

29. Халсалл Фред / Передача данных, сети компьютеров и взаимосвязь открытых систем, 1995. (дата звернення 01.05.2020)